UNIVERSIDADE ESTADUAL DA PARAÍBA - UEPB
CENTRO DE CIÊNCIAS HUMANAS E EXATAS - CCHE
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

Misaelle do Nascimento Oliveira

Resoluções de Equações de 5º grau Via Congruências

Monteiro - PB

2011

MISAELLE DO NASCIMENTO OLIVEIRA

Resoluções de Equações de 5º grau Via Congruências

Trabalho de Conclusão do Curso apresentado ao Centro de Ciências Humanas e Exatas - CCHE da Universidade Estadual da Paraíba - UEPB , em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática . sob a orientação do Professor Ms. Luiz Lima de Oliveira Junior.

Monteiro - PB
2011

FICHA CATALOGRÁFICA ELABORADA PELA BIB. SETORIAL – CAMPUS VI

O48r OLIVEIRA, Misaelle do Nascimento.

Resolução de Equações de 5º Grau Via Congruências/ Misaelle do Nascimento Oliveira. – 2011.

102f.

Digitado.

Trabalho acadêmico orientado (Graduação em Lic. Plena em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas, 2011.

"Orientação: Profº Ms. Luiz Lima de Oliveira Junior, Universidade Estadual da Paraíba – Campus VI".

1 Congruência. 2 Sistemas 3 Polinômios I. Título.

21. ed. CDD 512.7

MISAELLE DO NASCIMENTO OLIVEIRA

Resoluções de Equações de 5º grau Via Congruências

Trabalho de Conclusão do Curso apresentado ao Centro de Ciências Humanas e Exatas - CCHE da Universidade Estadual da Paraíba - UEPB , como pré-requisito para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática .

Aprovado pela banca examinadora em 15 de Junho de 2011.

Banca Examinadora

Prof. Ms. Luiz Lima de Oliveira Juniior
Dpto. Matemática - CCT/UEPB
EXAMINADOR

Prof. Ms.Luciano dos Santos Ferreira
Centro de Ciências Humanas e Exatas- CCHE/UEPB

Dedico este trabalho a minha família que sempre está me dando apoio no curso de graduação em matemática, em especial a meus pais, pelas angustias e preocupações que passaram por minha causa, por terem dedicado suas vidas a mim, pelo amor carinho e estimulo que me ofereceram, ao meu filho, que sem dúvida alguma, plantou em mim forças para que eu pudesse chegar ao fim, dedico-lhes essa conquista como gratidão.

Agradecimentos

Primeiramente, a Deus por este sonho realizado. Pelo dom da vida, pela fé e perseverança para vencer os obstáculos surgidos nesta fase da minha vida, a todos os professores que participaram da minha formação, em especial ao professor Luiz Lima de Oliveira Junior, que mim orientou e esteve ao meu lado durante esta última fase do curso, aos colegas que trilharam este caminho comigo e as pessoas que indiretamente com o seu carinho, contribuiram de forma significativa para este momento, a meus pais pelo apoio e carinho em todos os momentos nesta fase de meu curso de graduação.

Resumo

O presente trabalho tem por objetivo determinar soluções para equações de congruência de grau menor do que ou igual a 5, ou seja, encontrar soluções ou raízes de polinômios de 5^{o} grau via congruências. Como suporte à pesquisa, apresentamos inicialmente os conceitos básicos do tema, que se configuram como técnicas, definições e resultados primordiais para o desenvolvimento da pesquisa em tela. Posteriormente, citamos as congruências lineares e os sistemas lineares que servem para encontrar concomitantemente uma solução única para várias equações de congruência. Para o desenvolvimento do trabalho, adotamos uma metodologia na qual foram coletadas obras bibliográficas e documentos eletrônicos disponíveis na internet sobre o assunto. Após a sondagem, efetuamos uma pesquisa exploratória sobre o objeto a ser estudado, a fim de selecionarmos as que mais se adequavam a realização da monografia, que serviram como alicerça para concretização da mesma. Ao término do trabalho, concluímos que através do algoritmo é possível encontrar soluções para equações de congruência de grau menor que ou igual a 5. Contudo, vale ressaltar que não é possível, pelo mesmo algoritmo, determinar a quantidade das soluções.

Palavras chave: congruência, sistemas, polinômios.

Abstract

This study has the aim to determine solutions to equations of congruence of a degree less than or equal to 5, with other words; to find solutions or roots of polynomials of degree 5 by using congruencies. As a support for the research, in the beginning we introduce the basic concepts of the subject, which consists of technicals, definitions and essential results for the development of research in the screen. Later, we mention the linear congruencies and linear systems that serve simultaneously to find a single solution to various equations of congruence. For the development of the work, we adopt a methodology in which were collected bibliographic works and electronic documents available on the internet about this topic. After the survey, we made an exploratory investigation into the object to be studied, in order to select those that best fitted the study was undertaken, which served as the underpinning for achieving the same. Upon completion of the work, we conclude that through the algorithm it is possible to find solutions to equations of congruence of degree less than or equal to 5. However, it is worth to highlight that it is not possible to determine the number of solutions by using the same algorithm.

Keywords:congruence, systems, polynomials .

Sumário

Introdução

O grande interesse e a curiosidade em estudar a teoria dos números foram primordiais para a escolha do tema de minha pesquisa, por este motivo resolvi desenvolver um trabalho monográfico para aprofundar meus estudos e tentar entender melhor alguns resultados da teoria das congruências, em especial, as equações de grau maior que l, que, durante a graduação, não tive a oportunidade de estudá-la em maior profundidade, haja vista a grade curricular do curso de matemática.

O principal objetivo deste trabalho é encontrar soluções para equações de congruência que possuem grau maior que um, por meio de um algoritmo. Para tanto, é imprescindível um bom entendimento total ou de parte dos principais resultados da teoria das congruências, que foram estudadas em nível de graduação. Sendo assim, todos os resultados aqui utilizados foram demonstrados minuciosamente e podem ser encontrados nas referências indicadas ao final deste trabalho.

A maioria dos resultados aqui apresentados foram coletados dos estudos realizados em sala de aula na disciplina de introdução à teoria dos números e, os demais, foram coletados por meio do sistema eletrônico na internet. Uma vez reunida todas as pesquisas, foi organizado um estudo bibliográfico para fins de análise que, posteriormente, foram arranjadas em três capítulos.

No capítulo I, veremos noções importantes que são indispensáveis para uma melhor compreensão das congruências, bem como das suas propriedades. Relembraremos também o conceito de polinômios.

No Capítulo II, estudaremos as congruências lineares, bem como os procedimentos para encontrarmos soluções dos sistemas por elas formados.

No terceiro e último capítulo, partiremos para descobrir, através de um procedimento algorítmico, as soluções das equações não-lineares, ou seja, obter raízes de polinômios via congruência.

Finalizando o trabalho, temos as considerações finais, as referências utilizadas no desenvolvimento desta monografia e o apêndice A, que contém um breve resumo da vida e das obras publicadas de Karl Friedrich Gauss.

1 Definições e Resultados Fundamentais

Nesse Capítulo, veremos alguns resultados preliminares utilizados no desenvolvimento desta monografia e que servirão de base para uma melhor compreensão das equações de congruência de grau maior que um, onde citaremos algumas definições e resultados importantes da Teoria dos Números[1] e enunciaremos apenas os resultados essencias para o desenvolvimento do assunto central, os quais, foram utilizados nas construções de técnicas que desenvolvemos ao longo desta monografia.

1.1 Origem das Congruências

O precussor da teoria das congruências módulo um número inteiro m, bem como, da notação utilizada, foi Karl Friedrich Gauss,[2] que durante os seus primeiros anos de pesquisas desenvolveu idéias, que na sua maioria, estão reunidas em sua obra *Disquisitiones Arithmeticae*, publicada em 1801.

As despesas das impressões dos exemplares foram custeadas pelo Duque de Braunschweig (Alemanha), o então Príncipe e Lorde, Carl Wilhelm Ferdinand, que apadrinhava todas as despesas financeiras de Gauss, para que ele continuasse desenvolvendo seus trabalhos.

As *Disquisitiones Arithmeticae* estão divididas em sete partes:

1. Congruências em geral;
2. Congruências de primeiro grau;
3. Resto de Potências;
4. Congruências de segundo grau;
5. Formas quadráticas;

[1] ver nas referências [3] e [4] ou qualquer livro introdutório à Teoria dos Números.
[2] físico, matemático e astrônomo alemão nasceu em Brunswick (Alemanha) em 30 de abril de 1777.

6. Aplicações;
7. Divisões do Círculo.

Tendo em vista, a suma importância das *Disquisitiones Arithmeticae* para a teoria dos números, iremos fazer a seguir, uma síntese dos principais conteúdos que servem de conceitos básicos, porém, indispensáveis para o desenvolvimento deste trabalho.

Veremos inicialmente as seções 1 e 2.

Congruências em Geral e Congruências de Primeiro Grau

Os conceitos de congruência estão dispostos desde a primeira página, na qual, Gauss já introduz um novo símbolo e diz que:

"Se um número m divide a diferença $a-b$ (ou $b-a$) de dois números a e b sem resto, então a e b dizem-se congruentes módulo m." Gauss escreveu

$$a \equiv b \ (mod\, m)$$

e lemos: a é congruente com b módulo m.

A relação obtida é chamada de congruência; m é chamado de módulo da congruência; b é dito o resto de a módulo m e, contrariamente, a é dito resto de b módulo m.

No caso em que, $a-b$ não for divisível por m, dizemos que a é incongruente com b módulo m, isto é, a não é resto de b módulo m, nem tão pouco, b é resto de a módulo m.
Assim, a definição de $a \equiv b \ (mod\, m)$, resulta em uma igualdade do tipo $(a-b) = my$, onde y é um número inteiro.

A escolha do símbolo $\equiv$ foi feita a partir de uma analogia entre congruências e igualdades. Todavia, o primeiro conceito é mais inclusivo, pois, podemos considerar a igualdade uma congruência de módulo 0.

Em seguida, na segunda seção do seu trabalho, Gauss demonstrou o Teorema Fundamental da Aritmética, o Teorema Fundamental da Álgebra, dentre outros. O primeiro dos teoremas diz o seguinte:

Todo número natural maior que 1 (um) pode, exceto pela ordem dos fatores, ser escrito de uma e uma só maneira como produto de números primos.

Após ter provado o segundo, Gauss determinou $mdc(a,b)$ e o $mmc(a,b)$ de dois inteiros a e b. E, a partir daí, determinou a solubilidade das congruências lineares: Se $d = mdc(a,m)$, então a condição necessária e suficiente para que a congruência $ax \equiv b \ (mod\, m)$ seja solúvel é que $d|b$. Então, existem d diferentes soluções inteiras módulo m, ou seja, d soluções.

Congruências de Segundo Grau

Nas seções três e quatro, Gauss continuou com a teoria das congruências, só que desta vez, abordou as de grau superior. Em especial, a congruência binomial $x_n \equiv 1 \ (mod\, m)$ e disse:

Se p é um número primo e a é um número inteiro qualquer não divisível por p, então $a^{p-1} \equiv 1 \ (mod\, m)$.

Na quarta seção, escreve sobre a teoria dos Restos Quadráticos, que é uma das mais importantes, dentre as demais, em teoria dos números e, diz que:
"Um número a é chamado resto quadrático do número m se a congruência $X^2 \equiv a\ (mod\, m)$ tiver solução. Se a congruência não tiver solução, então a não é um resto quadrático de m."

1.2 Números Inteiros

Os números inteiros ou apenas os inteiros são:

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

cujo conjunto representa-se pela letra $\mathbb{Z}$, isto é:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Neste conjunto, destacam-se os seguintes subconjuntos:

(1) Conjunto $\mathbb{Z}^*$ dos inteiros não nulos:

$$\mathbb{Z}^* = \{x \in \mathbb{Z} | x \neq 0\} = \{\pm 1, \pm 2, \pm 3, \ldots\}$$

(2) Conjunto $\mathbb{Z}_+$ dos inteiros não negativos:

$$\mathbb{Z}_+ = \{x \in \mathbb{Z} | x \geq 0\} = \{0, 1, 2, 3, \ldots\}$$

(3) Conjunto $\mathbb{Z}_-$ dos inteiros não positivos:

$$\mathbb{Z}_- = \{x \in \mathbb{Z} | x \leq 0\} = \{0, -1, -2, -3, \ldots\}$$

(4) Conjunto $\mathbb{Z}_+^*$ dos inteiros positivos:

$$\mathbb{Z}_+^* = \{x \in \mathbb{Z} | x > 0\} = \{1, 2, 3, \ldots\}$$

(5) Conjunto $\mathbb{Z}_-^*$ dos inteiros negativos:

$$\mathbb{Z}_-^* = \{x \in \mathbb{Z} | x < 0\} = \{-1, -2, -3, \ldots\}.$$

Os inteiros positivos são também denominados inteiros naturais e por isso o conjunto dos inteiros positivos é habitualmente designado pela letra $\mathbb{N}(\mathbb{N} = \mathbb{Z}_+^*)$.

1.3 Propriedade dos Inteiros

O conjunto $\mathbb{Z}$ dos inteiros munido das operações de adição $(+)$ e multiplicação $(\cdot)$ possui as propriedades fundamentais que a seguir enumeramos, onde a, b e c são inteiros quaisquer, isto é, elementos de $\mathbb{Z}$:

(1) $a+b=b+a$ e $ab=ba$

(2) $(a+b)+c=a+(b+c)$ e $(ab)c=a(bc)$

(3) $0+a=a$ e $1.a=a$

(4) $-a=(-1)a$ e $a-a=a+(-a)=0$

(5) $a(b+c)=ab+ac$

(6) $0.a=0$, e se $ab=0$, então $a=0$ ou $b=0$.

Também existe uma "relação de ordem" entre os inteiros, representada pelo sinal "$<$ (*menor que*)", que possui as seguintes propriedades:

(7) Se $a\neq 0$, então $a<0$ ou $0<a$

(8) Se $a<b$ e $b<c$, então $a<c$

(9) Se $a<b$, então $a+c<b+c$

(10) Se $a<b$ e $0<c$, então $ac<bc$

(11) Se $a<b$ e $c<0$, então $bc<ac$

destas propriedades podem ser deduzidas muitas outras propriedades dos inteiros.

Exemplo 1.1. *Vamos mostrar que* $-(a+b)=(-a)+(-b)$.

Solução: Baseado nas propriedades supracitadas, temos sucessivamente:

$$-(a+b)=(-1)(a+b)= \qquad \text{(Propriedade 4)}$$

$$=(-1).a+(-1).b= \qquad \text{(Propriedade 5)}$$

$$=(-a)+(-b). \qquad \text{(Propriedade 4)}$$

Exemplo 1.2. *Demonstre que, se* $x\neq 0$*, então* $0<x^2$.

Demonstração.

Por hipótese, se $x\neq 0$, então $x<0$ ou $0<x$. (Propriedade 7)

Sendo assim, temos as seguintes condições:

Se $x<0$, então $0.x<x.x$ (Propriedade 11)

$$0<x^2 \qquad \text{(Propriedade 6)}$$

Se $0<x$, então $0.x<x.x$ (Propriedde 10)

$$0<x^2. \qquad \text{(Propriedade 6)}$$

Princípio da Boa Ordenação

Definição 1.1 (PBO). *Todo conjunto não vazio A, de inteiros não negativos, contém um elemento mínimo.*

Em outros termos, todo subconjunto não vazio A do conjunto $\mathbb{Z}_+ = \{0, 1, 2, 3, \ldots\}$ dos inteiros não negativos $(\emptyset \neq A \subset \mathbb{Z}_+)$ possui o elemento mínimo.

Exemplo 1.3. *O conjunto $A = \{1, 3, 5, 7, \ldots\}$ dos inteiros positivos ímpares é um subconjunto não vazio de $\mathbb{Z}_+ (\emptyset \neq A \subset \mathbb{Z}_+)$. Logo, pelo "Princípio da Boa Ordenação", A possui o elemento mínimo $(min(A) = 1)$.*

Teorema 1.1. *(de Arquimedes)*[3] *Se a e b são dois inteiros positivos quaisquer, então existe um inteiro positivo n tal que $na \geq b$.*

Prova. Suponhamos que a e b são dois inteiros positivos para os quais $na < b$ para todo inteiro positivo n. Então, todos os elementos do conjunto:

$$S = \{b - na \,|\, n \in \mathbb{N}\}$$

são inteiros positivos e, pelo Princípio da Boa Ordenação, S possui o elemento mínimo, digamos $min\,(S) = b - ka$. E como $b - (k+1)a$ pertence a S, porque S contém todos os inteiros positivos desta forma, temos:

$$b - (k+1)a = b - (ka + a) = b + (-ka - a) = (b - ka) - a < b - ka,$$

isto é, $b - ka$ não é o elemento mínimo de S, o que é uma contradição. Logo, a propriedade arquimediana é verdadeira. ■

Exemplo 1.4. *Dados os inteiros a e b, vamos encontrar um $n \in \mathbb{Z}$ tal que $n \cdot a \geq b$.*

Solução:

(i) *Se $a = 2$ e $b = 11$, então $n = 6$, porque $6.2 > 11$:*

(ii) *Se $a = 9$ e $b = 5$, então $n = 1$, porque $1.9 > 5$.*

1.4 Princípio de Indução Finita

Teorema 1.2 (Indução Finita). *Seja S um subconjunto do conjunto $\mathbb{Z}_+^* (S \subset \mathbb{Z}_+^*)$ que satisfaz as duas seguintes condições:*

(1) *1 pertence a* S *$(1 \in S)$;*

(2) *para todo inteiro positivo* k, *se $k \in S$, então $k + 1 \in S$.*

Nestas condições, S *é o conjunto $\mathbb{Z}_+^*$ dos inteiros positivos: $S = \mathbb{Z}_+^*$.*

[3] matemático, físico, engenheiro, inventor, e astrônomo grego. Nascido em Siracusa-Sicília, por volta do ano 287 a.C

Prova. Iremos demonstrar este teorema por contradição.

Considere que S não seja o conjunto $\mathbb{Z}_+^*$ dos inteiros positivos ($S \neq \mathbb{Z}_+^*$). Seja X o conjunto de todos os inteiros positivos que não pertencem a S, isto é:

$$X = \left\{ x \,|\, x \in \mathbb{Z}_+^* \text{ e } x \notin S \right\} = \mathbb{Z}_+^* - S.$$

Então, X é um subconjunto não vazio de $\mathbb{Z}_+^*$ ($\emptyset \neq X \subset \mathbb{Z}_+^*$) e pelo *"Princípio da boa ordenação,"* existe o elemento mínimo que é, x_0 de X ($min X = x_0$).

Pela condição (1), $1 \in S$ de modo que $x_0 > 1$ e, portanto, $x_0 - 1$ é um inteiro positivo que não pertence a X. Logo, $x_0 - 1 \in S$ e pela condição (2), segue-se que $(x_0 - 1) + 1 = x_0 \in S$, o que é um absurdo, pois, como dissemos inicialmente, $x_0 \in X = \mathbb{Z}_+^* - S$, isto é, $x_0 \notin S$. Assim sendo, $X = \emptyset$ e $S = \mathbb{Z}_+^*$.

Todavia, de acordo com este *"Princípio de indução finita"*, o único subconjunto de $\mathbb{Z}_+^*$ que satisfaz às condições (1) e (2) é o próprio $\mathbb{Z}_+^*$. ■

1.5 Máximo Divisor Comum de Dois Inteiros

Definição 1.2 (Divisor)**.** *Sejam a e b dois inteiros, sendo $a \neq 0$. Dizemos que a divide b se, e somente se, existe um inteiro q tal que $b = aq$.*

Da definição obtemos o seguinte: a é dito divisor de b ou fator de b, por outro lado, b é um múltiplo de a ou b é divisível por a.

Exemplo 1.5. *Dado os números 6, 30, -28, e 35, vamos verificar se 2, -5, 7 e 10 são seus respectivos divisores.*

Solução:
$2|6$, pois $6 = 2 \cdot 3$
$-5|30$, pois $30 = (-5) \cdot (-6)$
$7|-28$, pois $-28 = 7 \cdot (-4)$
$10 \nmid 35$, porque não existe $q \in \mathbb{Z}$ tal que $35 = 10q$.

Definição 1.3. *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se máximo divisor comum de a e b o inteiro positivo d ($d > 0$) que satisfaz às condições:*

(1) $d|a$ e $d|b$
(2) se $c|a$ e se $c|b$, então $c \leq d$.

Observe-se que, pela condição (1), d é um divisor comum de a e b, e pela condição (2), d é o maior dentre todos os divisores comuns de a e b.

O máximo divisor comum de a e b indica-se pela notação $mdc(a,b)$.

É imediato que o $mdc(a,b) = mdc(b,a)$. Em particular,

(i) o $mdc\,(0,0)$ não existe
(ii) o $mdc\,(a,1)=1$
(iii) se $a\neq 0$, então o $mdc\,(a,0)=|a|$
(iv) se $a|b$, então o $mdc\,(a,b)=|a|$

Exemplo 1.6. *Obtenha o máximo divisor comum dos seguintes inteiros: 9 e 1, -5 e 0, -8 e 16.*

Solução:
$mdc\,(9,1)=1$,
$mdc\,(-5,0)=|-5|=5$
$mdc\,(-8,16)=|-8|=8$

Exemplo 1.7. *Sejam os inteiros $a=16$ e $b=24$. Os divisores comuns positivos de 16 e 24 são 1, 2, 4 e 8, e como o maior deles é 8, segue-se que o $mdc\,(16,24)=8$.*

Observa-se que:
$mdc\,(-16,24)=mdc\,(16,-24)=mdc\,(-16,-24)=8$.

Exemplo 1.8. *Sejam os inteiros $a=-15$ e $b=45$. Os divisores comuns positivos de -15 e 45 são 1, 3, 5 e 15 e, como o maior deles é 15, segue-se que o $mdc\,(-15,45)=15$.*

Existência e Unicidade do MDC

Teorema 1.3. *Se a e b são dois inteiros não conjuntamente nulos ($a\neq 0$ ou $b\neq 0$), então existe e é único o mdc (a, b); além disso, existem inteiros x e y tais que*

$$mdc\,(a,b)=ax+by,$$

isto é, o $mdc\,(a,b)$ é uma combinação linear[4] *de a e b.*

Prova. Seja L o conjunto de todos os inteiros positivos da forma $ax+by$, com $x, y\in\mathbb{Z}$, isto é:

$$L=\{ax+by\,|\,ax+by>0 \text{ e } x,y\in\mathbb{Z}\}.$$

Este conjunto L não é vazio ($L\neq\emptyset$), porque por exemplo, se $a\neq 0$, então um dos dois inteiros

$$a=a.1+b.0 \qquad \text{e} \qquad -a=a.(-1)+b.0$$

é positivo e pertence a L. Logo, pelo *"Princípio da Boa Ordenação"*, existe e é único o elemento mínimo d de L, ou seja, $minL=d>0$. E, como d pertence a L, existem inteiros x e y tais que $d=ax+by$. Vamos mostrar que $d=mdc\,(a,b)$.

[4] Sendo $d=mdc(a,b)$, existem $x, y\in\mathbb{Z}$ tais que d é o menor inteiro positivo da forma $ax+by$

Com efeito, pelo algoritmo da divisão[5], temos

$$a = d \cdot q + r, \quad \text{com } 0 \leq r < d$$

daí

$$r = a - d \cdot q = a - (ax + by) \cdot q = a - (aq \cdot x + bq \cdot y) =$$

$$= (a - aq \cdot x) - bq \cdot y = a \cdot (1 - q \cdot x) + b \cdot (-q \cdot y)$$

isto é, o resto r é uma combinação linear de a e b. Como $0 \leq r < d$ e $d > 0$ é o elemento mínimo de L, segue que $r = 0$ e $a = d \cdot q$, isto é, $d|a$. Analogamente, concluímos que $d|b$. Logo, d é um divisor comum positivo de a *e* b. E se c é um divisor comum positivo qualquer de a *e* b, então ($c|a$ e $c|b$, $c > 0$), então:

$$c|(ax + by) \Longrightarrow c|d \Longrightarrow c \leq d$$

isto é, d é o maior divisor comum positivo de a e b, ou seja,

$$mdc\,(a, b) = d = ax + by, \quad x, y \in \mathbb{Z}$$

o que conclui a demonstração deste teorema. ■

1.6 Mínimo Múltiplo Comum de Dois Inteiros

Definição 1.4. *Sejam a e b dois inteiros diferentes de zero* ($a \neq 0 e b \neq 0$). *Chama-se mínimo múltiplo comum de a e b o inteiro positivo* $m\,(m > 0)$ *que satisfaz às condições:*

(1) $a|m$ e $b|m$

(2) se $a|c$ e se $b|c$, com $c > 0$, então $m \leq c$.

Observe-se que, pela condição (1), m é um múltiplo comum de a e b, e pela condição (2), m é o menor dentre todos os múltiplos comuns positivos de a e b.

O mínimo múltiplo comum de a e b indica-se pela notação $mmc\,(a, b)$.

Pelo Princípio da boa ordenação, o conjunto dos múltiplos comuns positivos de a e b possui o elemento minímo e, portanto, o $mmc\,(a, b)$ existe sempre e é único. Além disso, por ser o produto ab um múltiplo comum de a e b, segue-se que o $mmc\,(a,b) \leq |ab|$. Em particular, se $a|b$, então o $mmc\,(a,b) = |b|$.

Exemplo 1.9. *Sejam os inteiros* $a = -12 e b = 30$. *Os múltiplos comuns positivos de -12 e 30 são 60, 120, 180, ..., e como o menor deles é 60, segue-se que o* $mmc\,(-12, 30) = 60$.

[5] ver seção 6.1 da referência [4]

1.7 Inteiros Primos e Primos entre si

Definição 1.5. *Diz-se que um inteiro positivo $p > 1$ é um número primo ou apenas um primo, se e somente se, 1 e p são os seus únicos divisores positivos. Um inteiro positivo maior que 1 e que não é primo diz-se composto.*

Exemplo 1.10. *Os inteiros positivos 2, 3, 5 e 7 são todos primos e os inteiros positivos 4, 6, 8 e 10 são todos compostos.*

Observação 1: O inteiro positivo 1 não é nem primo nem composto e, por conseguinte, se a é um inteiro positivo qualquer, então a é primo, a é composto ou $a = 1$.

Observação 2: Observe que 2 é o único inteiro positivo par, que é primo.

Definição 1.6. *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0 ou b \neq 0$). Diz-se que a e b são primos entre si, se e somente se o $mdc(a,b) = 1$.*

Exemplo 1.11. *São primos entre si os inteiros: 3 e 5, -8 e 19, -27 e -10, pois temos: $mdc(2,5) = mdc(-9,16) = mdc(-27,-35) = 1$.*

Dois inteiros a e b primos entre si admitem como únicos divisores comuns 1 e -1.

Teorema 1.4. *Dois inteiros a e b, não conjuntamente nulos ($a \neq 0 ou b \neq 0$), são primos entre si, se e somente se, existem inteiros x e y tais que $ax + by = 1$.*

Prova. ($\Longrightarrow$) Se a eb são primos entre si, então o $mdc(a,b) = 1$ e por conseguinte existem inteiros x e y tais que $ax + by = 1$.

($\Longleftarrow$) Reciprocamente, se existem inteiros x e y tais que $ax + by = 1$ e se o $mdc(a,b) = d$, então $d|a e d|b$. Logo, $d|(ax + by)$ e $d|1$, o que implica $d = 1$ ou $mdc(a,b) = 1$, isto é, a e b são primos entre si. ■

Corolário 1.1. *Se o $mdc(a,b) = d$, então o $mdc(a/d, b/d) = 1$.*

Prova. Primeiramente, observe que a/d e b/d são inteiros, porque d é um divisor comum de $a e b$.

Posto isto, se o $mdc(a,b) = d$, então existem inteiros x e y tais que

$$ax + by = d,$$

ou seja, dividindo ambos os membros desta igualdade por d:

$$(a/d)x + (b/d)y = 1.$$

Logo, pelo teorema anterior, os inteiros a/d e b/d são primos entre si, isto é, o $mdc(a/d, b/d) = 1$. ■

Exemplo 1.12. *O* $mdc\,(-12, 30) = 6$ *e o* $mdc\,(-12/6, 30/6) = mdc\,(-2, 5) = 1$

Teorema 1.5. *(de EUCLIDES)*[6] *Se* $a|bc$ *e se o* $mdc\,(a,b) = 1$, *então* $a|c$.

Prova. Queremos mostrar que, dado $a|bc$ se a e b são primos entre si, então $a|c$. Assim sendo, temos:

$a|bc \Longrightarrow bc = aq, \quad \text{com} \quad q \in \mathbb{Z}.$

Como o $mdc\,(a,b) = 1 \Longrightarrow ax + by = 1. \qquad \text{com} \quad x, y \in \mathbb{Z}$

$\Longrightarrow acx + bcy = c.$

Portanto:

$$c = acx + aqy = a(cx + qy) \Longrightarrow a|c.$$

■

Note que somente a condição $a|bc$ não implica que $a|c$.

Exemplo 1.13. *Observe que* $12|9.8$, *mas* $12 \nmid 9$ *e* $12 \nmid 8$ *e o* $mdc\,(12,9) \neq 1$ *e* $mdc\,(12,8) \neq 1$.

1.8 Inteiros Congruentes

Definição 1.7. *Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo fixo. Dizemos que a é congruente a b módulo m se, e somente se, m divide a diferença* $a - b$.

Em outros termos, a é congruente a b módulo m se, e somente se, existe um inteiro k tal que $a - b = km$. Com a notação

$$a \equiv b \ (mod\, m)$$

indica-se que a é congruente a b módulo m. Portanto, simbolicamente:

$$a \equiv b \ (mod\, m) \Longleftrightarrow m|(a-b)$$

ou seja:

$$a \equiv b \ (mod\, m) \Longleftrightarrow \exists k \in \mathbb{Z} \text{tal que} \, a - b = km.$$

Exemplo 1.14. *Observe que:*

$3 \equiv 24 \ (mod\, 7)$, *pois* $7|(3-24)$

$-31 \equiv 11 \ (mod\, 6)$, *pois que* $6|(-31-11)$

$-15 \equiv -63 \ (mod\, 8)$, *pois* $8|(-15-(-63))$

Se m não divide a diferença $a - b$, então dizemos que a é incongruente a b módulo m, o que se indica pela notação:

$$a \not\equiv b \ (mod\, m).$$

[6] Matemático grego, viveu em Alexandria na primeira metade do séc. III a.C.

Exemplo 1.15. *Dado os números: 25 e 12, -21 e 10, 16 e 9 constate se algum deles, são ou não, congruentes módulo 7, 5 e 4 respectivamente.*

Solução:
$25 \not\equiv 12\ (mod\, 7)$, porque $7 \nmid (25-12)$
$-21 \not\equiv 10\ (mod\, 5)$, porque $5 \nmid (-21-10)$
$16 \not\equiv 9\ (mod\, 4)$, porque $4 \nmid (16-9)$.

Observação 3: note que dois inteiros quaisquer são congruentes módulo 1, enquanto que dois inteiros são congruentes módulo 2 se ambos são pares ou se ambos são ímpares.

Em particular, $a \equiv 0\ (mod\, m)$ se, e somente se, o módulo m divide a $(m-a)$.

Exemplo 1.16. *Mostrar:*

$$n \equiv 7\ (mod\, 12) \Longrightarrow n \equiv 3\ (mod\, 4), \qquad \forall\, n \in \mathbb{Z}$$

Solução:
$n \equiv 7\ (mod\, 12) \Longrightarrow n-7 = 12k \Longrightarrow n-3-4 = 12k \Longrightarrow n-3 = 12k+4 \Longrightarrow n-3 = 4(3k+1) \Longrightarrow 4|(n-3) \Longrightarrow n \equiv 3\ (mod\, 4)$.

Exemplo 1.17. *Resolver as equações de congruências:*

$$n^2 \equiv 0\ (mod\, 4) \qquad ou \qquad n^2 \equiv 1\ (mod\, 4), \qquad \forall n \in \mathbb{Z}$$

Solução: Vamos considerar, inicialmente,
n par: $n = 2k \Longrightarrow n^2 = (2k)^2 \Longrightarrow n^2 = 4k^2 \Longrightarrow 4|n^2$
$\Longrightarrow n^2 \equiv 0\ (mod\, 4)$.
Agora vamos considerar,
n ímpar: $n = 2k+1 \Longrightarrow n^2 = (2k+1)^2 \Longrightarrow n^2 = 4(k^2+k)+1 \Longrightarrow n^2-1 = 4(k^2+k)$
$\Longrightarrow 4|(n^2-1) \Longrightarrow n^2 \equiv 1\ (mod\, 4)$.

Caracterização de Inteiros Congruentes

Teorema 1.6. *Dois inteiros a e b são congruentes módulo m se, e somente se, a e b deixam o mesmo resto quando divididos por m*

Prova. $(\Longrightarrow)$ Suponhamos que $a \equiv b\ (mod\, m)$. Então, por definição:
$a-b = km$, com $k \in \mathbb{Z}$
Seja r o resto da divisão de b por m; então, pelo *algoritmo da divisão:*

$$b = mq + r, \quad \text{onde} \quad 0 \leq r < m$$

portanto,

$$a-b = km \Longrightarrow a = km+b = km+mq+r = (k+q)m+r$$

e isto significa que r é o resto da divisão de a por m, isto é, os inteiros a e b divididos por m deixam o mesmo resto r.

($\Longleftarrow$)Reciprocamente, suponhamos que a e b divididos por m deixam o mesmo resto r. Então, podemos escrever:

$$a = mq_1 + r \quad \text{e} \quad b = mq_2 + r, \qquad \text{onde} \quad 0 \leq r < m$$

e portanto:

$$a - b = (mq_1 + r) - (mq_2 + r) = mq_1 - mq_2 = m(q_1 - q_2) \Longrightarrow m|(a-b) \Longrightarrow a \equiv b \ (mod\, m).$$

■

Exemplo 1.18. *Sejam os inteiros* -56 *e* -11. *Pelo algoritmo da divisão:*[7]

$$-56 = 9(-7) + 7 \quad e \quad -11 = 9(-2) + 7$$

isto é, -56 e -11 divididos por 9 deixam o mesmo resto 7. *Logo, pelo teorema anterior:* $-56 \equiv -11 \ (mod\, 9)$.

Sejam agora, os inteiros -31 e 11. Temos a congruência:

$$-31 \equiv 11 \ (mod\, 7)$$

de modo que, pelo teorema anterior, -31 e 11 divididos por 7 deixam o mesmo resto. Realmente, é o que mostram as igualdades:

$$-31 = 7(-5) + 4 \quad \text{e} \quad 11 = 7.1 + 4.$$

Propriedade das Congruências

Teorema 1.7. *Seja m um inteiro positivo fixo* $(m > 0)$ *e sejam a, b e c inteiros quaisquer. Subsistem as seguintes propriedades:*

(1) $a \equiv a \ (mod\, m)$

(2) Se $a \equiv b \ (mod\, m)$, então $b \equiv a \ (mod\, m)$

(3) Se $a \equiv b \ (mod\, m)$ e se $b \equiv c \ (mod\, m)$, então $a \equiv c \ (mod\, m)$.

Prova. (1) Com efeito:

$$m|0 \text{ ou } m|(a-a) \Longrightarrow a \equiv a \ (mod\, m).$$

(2) Com efeito, se $a \equiv b \ (mod\, m)$, então $a - b = km$, com $k \in \mathbb{Z}$.

[7] Idem, p.20

Portanto:

$$b-a=-(km)=(-k)m \Longrightarrow b \equiv a \ (mod\, m).$$

(3) Com efeito, se $a \equiv b \ (mod\, m)$ e se $b \equiv c \ (mod\, m)$, então existem inteiros h e k tais que

$$a-b=hm \text{ e } b-c=km.$$

Portanto:

$$a-c=(a-b)+(b-c)=hm+km=(h+k)m$$

e isto significa que $a \equiv c \ (mod\, m)$. ■

NOTA: Podemos ver que neste teorema, a relação R no conjunto $\mathbb{Z}$ dos inteiros definida por

$$aRb \Longleftrightarrow a \equiv b \ (mod\, m),$$

é reflexiva, simétrica e transitiva, ou seja, R é uma relação de equivalência em $\mathbb{Z}$.

Esta relação de equivalência R em $\mathbb{Z}$ é denominada *"congruência módulo m"*.

Teorema 1.8. *Seja m um inteiro positivo fixo* $(m>0)$*e sejam a e b dois inteiros quaisquer. Subsistem as seguintes propriedades:*

(1) Se $a \equiv b \ (mod\, m)$ e se $n|m$, com $n>0$, então $a \equiv b \ (mod\, n)$

(2) Se $a \equiv b \ (mod\, m)$ e se $c>0$, então $ac \equiv bc \ (mod\, mc)$

(3) Se $a \equiv b \ (mod\, m)$ e se a, b, m são todos divisíveis pelo inteiro $d>0$, então $a/d \equiv b/d \ (mod\, m/d)$.

Prova. (1) Com efeito:

$a \equiv b \ (mod\, m) \Longrightarrow a-b=km$ e $n|m \Longrightarrow m=nq$ onde k e $q>0$ são inteiros.

Portanto:

$$a-b=(kq)n \Longrightarrow a \equiv b \ (mod\, n).$$

(2) Com efeito:

$$a \equiv b \ (mod\, m) \Longrightarrow a-b=km \Longrightarrow ac-bc=k(mc) \Longrightarrow ac \equiv bc \ (mod\, mc).$$

(3) Com efeito:

$$a \equiv b \ (mod\, m) \Longrightarrow a-b=km \Longrightarrow a/d-b/d=k(m/d) \Longrightarrow a/d \equiv b/d \ (mod\, m/d).$$

■

Exemplo 1.19. *Dada as congruências, observe a relação entre elas:*

$-15 \equiv 9 \ (mod\, 8) \Longrightarrow -15 \equiv 9 \ (mod\, 4)$

$7 \equiv -8 \ (mod\, 3) \Longrightarrow 35 \equiv -40 \ (mod\, 15)$

$36 \equiv -24 \ (mod\, 12) \Longrightarrow 9 \equiv -6 \ (mod\, 3)$

Teorema 1.9. *Seja m um inteiro positivo fixo $(m > 0)$ e sejam a, b, c, d inteiros quaisquer. Subsistem as seguintes propriedades:*
(1) *Se $a \equiv b \pmod m$ e se $c \equiv d \pmod m$, então $a+c \equiv b+d \pmod m$ e $ac \equiv bd \pmod m$*
(2) *Se $a \equiv b \pmod m$, então $a+c \equiv b+c \pmod m$ e $ac \equiv bc \pmod m$*
(3) *Se $a \equiv b \pmod m$, então $a^n \equiv b^n \pmod m$ para todo inteiro positivo n.*

Prova. (1) Com efeito, se $a \equiv b \pmod m$ e se $c \equiv d \pmod m$, então existem inteiros h e k tais que $a-b = hm$ e $c-d = km$. Portanto:

$$(a+c)-(b+d) = (a-b)+(c-d) = hm+km = (h+k)m$$

e

$$ac-bd = (b+hm)(d+km)-bd = (bk+dh+hkm)m$$

o que implica:

$$a+c \equiv b+d \pmod m \text{ e } ac \equiv bd \pmod m.$$

(2) Com efeito, se $a \equiv b \pmod m$, como $c \equiv c \pmod m$, temos pela propriedade anterior:

$$a+c \equiv b+c \pmod m \text{ e } ac \equiv bc \pmod m.$$

(3) Usando indução, a proposição é verdadeira para $n = 1$, e suponha ser verdadeira para um inteiro positivo k, temos:

$$a^k \equiv b^k \pmod m \text{ e } a \equiv b \pmod m.$$

Portanto, pela propriedade (1):

$$a^k \cdot a \equiv b^k \cdot b \pmod m \qquad \text{ou} \qquad a^{k+1} \equiv b^{k+1} \pmod m$$

isto é, a proposição é verdadeira para o inteiro positivo $k+1$. Logo, a proposição é verdadeira para todo inteiro positivo n. ■

Exemplo 1.20. (i) $12 \equiv 22 \pmod 5$ *e* $8 \equiv 13 \pmod 5$ *implica:*
$12+8 \equiv 22+13 \pmod 5$ *ou* $20 \equiv 35 \pmod 5$
e
$12.8 \equiv 22.13 \pmod 5$ *ou* $96 \equiv 286 \pmod 5$
(ii) $12 \equiv 5 \pmod 7$ *implica:*
$12+6 \equiv 5+6 \pmod 7$ *ou* $18 \equiv 11 \pmod 7$
e
$12(-9) \equiv 5(-9) \pmod 7$ *ou* $-108 \equiv -45 \pmod 7$
(iii) $-5 \equiv 2 \pmod 7$ *implica:*

$$(-5)^3 \equiv 2^3 \ (mod\, 7) \qquad ou \qquad -125 \equiv 8 \ (mod\, 7).$$

Exemplo 1.21. *Mostrar que* $a \equiv b \ (mod\, m)$ *implica* $-a \equiv -b \ (mod\, m)$.

Solução: Com efeito, multiplicando ordenadamente as congruências:

$$a \equiv b \ (mod\, m) \qquad \text{e} \qquad -1 \equiv -1 \ (mod\, m)$$

obtemos,

$$a(-1) \equiv b(-1) \ (mod\, m) \qquad \text{ou} \qquad -a \equiv -b \ (mod\, m).$$

Exemplo 1.22. *Mostrar que* $a+b \equiv c \ (mod\, m)$ *implica* $a \equiv c-b \ (mod\, m)$.

Solução: Com efeito, somando ordenadamente as congruências:

$$a+b \equiv c \ (mod\, m) \qquad \text{e} \qquad -b \equiv -b \ (mod\, m)$$

obtemos,

$$a+b+(-b) \equiv c+(-b) \ (mod\, m) \qquad \text{ou} \qquad a \equiv c-b \ (mod\, m).$$

Observação 4: Em uma congruência podemos passar um termo de um membro para o outro trocando o sinal.

Teorema 1.10. *Se* $ac \equiv bc \ (mod\, m)$ *e se o* $mdc(c,m) = d$*, então* $a \equiv b \ (mod\, m/d)$.

Prova. Com efeito, se $ac \equiv bc \ (mod\, m)$, então:

$$ac - bc = (a-b)c = km, \quad \text{com } k \in \mathbb{Z}$$

e se o $mdc(c,m) = d$, existem inteiros r e s tais que $c = dr$ e $m = ds$, onde r e s são primos entre si. Portanto:

$$(a-b)dr = kds \qquad \text{ou} \qquad (a-b)r = ks$$

o que implica que $s|(a-b)r$, com o $mdc(r,s) = 1$. Logo, pelo teorema 1.6 (de EUCLIDES): $s|(a-b) \quad \text{e} \quad a \equiv b \ (mod\, s)$ ou, por ser $s = m/d$, $a \equiv b \ (mod\, m/d)$. ■

Corolário 1.1. *Se* $ac \equiv bc \ (mod\, m)$ *e se o* $mdc(c,m) = 1$*, então* $a \equiv b \ (mod\, m)$.

Prova. De acordo com o teorema anterior, se $ac \equiv bc \ (mod\, m)$ então $ac - bc = (a-b)c = km$, com $k \in \mathbb{Z}$. Por hipótese, o $mdc(c,m) = 1$, como m divide o produto $(a-b).c$, concluímos que $m|(a-b)$ e portanto $a \equiv b \ (mod\, m)$.

Esta propriedade mostra que é permitido cancelar fatores de ambos os membros de uma congruência que são primos com o módulo. ■

Corolário 1.2. *Se $ac \equiv bc \ (mod\, p)$, com p primo, e se p não divide c $(p \nmid c)$, então $a \equiv b \ (mod\, p)$.*

Prova. Com efeito, as condições: p é primo e p não divide c $(p \nmid c)$, implica que o $mdc(c,p) = 1$. Da equação enunciada, temos $ac - bc = (a-b)c = kp$, com $k \in \mathbb{Z}$, consequentemente $p|(a-b)$, portanto $a \equiv b \ (mod\, p)$. ■

Exemplo 1.23. *Consideremos a congruência:*

$$33 \equiv 15 \ (mod\, 9) \qquad \text{ou} \qquad 3.11 \equiv 3.5 \ (mod\, 9)$$

como o $mdc(3,9) = 3$, pelo teorema 1.11, temos: $11 \equiv 5 \ (mod\, 3)$.

Exemplo 1.24. *Consideremos a congruência:*

$$-35 \equiv 45 \ (mod\, 8) \qquad \text{ou} \qquad 5(-7) \equiv 5.9 \ (mod\, 8)$$

como o $mdc(5,8) = 1$, podemos cancelar o fator 5 de ambos os membros da congruência, o que dá a nova congruência: $-7 \equiv 9 \ (mod\, 8)$.

Observação 5: Na congruência $4.11 \equiv 4.15 \ (mod\, 8)$ não podemos cancelar o fator 4, porque o $mdc(4,8) = 4 \neq 1$. Realmente, $11 \not\equiv 15 \ (mod\, 8)$. Mas, temos $11 \equiv 15 \ (mod\, 2)$.

1.9 Polinômios

Definição 1.8. *Seja A um conjunto não-vazio onde duas operações "+" e "$\cdot$" estão definidas. Dizemos que $(A, +, \cdot)$ é um "anel" quando as seguintes condições são satisfeitas:*

(A1) $(A, +)$ é um grupo abeliano.
Sendo assim, subsistem as seguintes propriedade:
existe $e \in A$ tal que $e * a = a * e = a$ para todo $a \in A$ (elemento neutro);
$a_1 * (a_2 * a_3) = (a_1 * a_2) * a_3$ para quaisquer $a_1, a_2, a_3 \in A$ (associatividade);
Para todo $a \in A$ existe $a^{-1} \in A$ tal que $a * a^{-1} = a^{-1} * a = e$ (elemento inverso).
Para quaisquer $a_1, a_2 \in A$, $a_1 * a_2 = a_2 * a_1$ (comutatividade);

Para quaisquer $a_1, a_2, a_3 \in A$, temos:

(A2) $a_1 \cdot (a_2 + a_3) = a_1 \cdot a_2 + a_1 \cdot a_3$, e $(a_1 + a_2) \cdot a_3 = a_1 \cdot a_3 + a_2 \cdot a_3$.

(A3) $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$.

Definição 1.9. *Seja A um anel qualquer. Definimos um polinômio sobre A na variável x como sendo uma expressão formal do tipo*

$$p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_mx^m + \ldots$$

onde $a_i \in A$ *para todo* $i \in \mathbb{N} \cap \{0\}$ *e existe* $N \in \mathbb{Z}_+$ *tal que* $a_i = 0$ *para todo* $i \geq N$.

O polinômio

$$p(x) = 0 + 0x + 0x^2 + \ldots + 0x^m + \ldots$$

é chamado polinômio nulo sobre A e será indicado simplesmente por $p(x) = 0$.

Todavia, se

$$p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_mx^m + \ldots$$

e se $n \in \mathbb{N} \cup \{0\}$ *possui o termo* $a_n \neq 0$ *e na sequência os termos* $a_{n+i} = 0$, *para todo* $i \in \mathbb{N}$ *então podemos escrever* $p(x)$ *assim:*

$$p(x) = a_0 + a_1x + \ldots + a_nx^n$$

e indicamos que o grau de $p(x)$ *é* n, *ou seja,* $gr(p) = n$.

Exemplo 1.25. *Vamos determinar o grau de cada polinômio* $f(x) = 4 + 7x + 2x^3 - 6x^4$ *e* $h(x) = 1 + 5x + -3x^2 + (a-4)x^3$

Solução:

Como já vimos, por definição o grau de $f(x)$ *é* $gr(f) = 4$ *e para determinarmos o grau de* $h(x)$ *precisamos observar o seguinte:* $gr(h) = 2$, *se* $a = 4$ *e* $gr(h) = 3$, *se* $a \neq 4$.

Teorema 1.11. *(***Fatoração***): Sejam* $f(x) \in \mathbb{Z}[x]$ *e* $a \in \mathbb{Z}$. *Então a é raiz de* $f(x)$ *módulo* $m \Leftrightarrow$ $f(x)$ *é divisível por* $(x-a)$ *módulo m.*

Prova. Vamos supor que $f(x) = b_kx^k + \ldots + b_1x + b_0$. Como

$$\begin{aligned}(x^m - a^m) &= (x-a)(x^{m-1} + ax^{m-2} + a^2x^{m-3} + \ldots + a^{m-1}) \\ &= (x-a)\,g_n(x), \quad \text{para todo } n \in \mathbb{N},\end{aligned}$$

podemos observar que $(x^m - a^m)$ é divisível por $(x-a)$ e portanto o resto $r(x) = 0$ é denominado de polinômio nulo.

Todavia, o resto de $f(x)$ é dado por $r = f(a)$, onde a é raiz de $f(x)$, logo

$$f(x) - f(a) = \sum_{i=1}^{k} b_i(x^i - a^i) = (x-a)\sum_{i=1}^{k} b_ig_i(x).$$

Assim temos que $f(x) - f(a) = (x-a)h(x)$. Em particular $f(x) \equiv (x-a)h(x)\ (mod\, m)$, pois por hipótese, $f(a) \equiv 0\ (mod\, m)$.

Reciprocamente, se $f(x)$ é divisível por $(x-a)$ módulo m então existe $g(x) \in \mathbb{Z}[x]$ tal que

$$f(x) \equiv (x-a)g(x) \ (mod\, m)$$

e daí é óbvio que $f(a) \equiv 0 \ (mod\, m)$. ■

Exemplo 1.26. *Dados os polinômios* $f(x) = x^5 - 4x^4 - 3x^2 + 7x - 1$ *e* $g(x) = x - 1$ *verifique se* $f(x)$ *é divisível por* $g(x)$.

Solução:

Com efeito, se $f(x)$ *é divisível por* $g(x)$ *então 1 é raiz de* $f(x)$*, logo,* $f(1) = 1^5 - 4.1^4 - 3.1^2 + 7.1 - 1 = 0$ *e concluímos que g divide* f.

2 Equações de Congruência

Começaremos este capítulo com o estudo de equações de congruências de grau um e apresentaremos o caso, no qual, a equação abrange mais de uma variável. Depois de apresentar minuciosamente todas as suas definições e demonstrações, veremos os sistemas lineares que envolvem estas equações, bem como indicaremos o procedimento de resolução dos mesmos. Em seguida, ilustraremos o presente conteúdo com exemplos que melhor esclareçam o entendimento por parte do leitor.

2.1 Equações de Grau Um

Neste parágrafo vamos iniciar o estudo da equações de congruência propriamente dito. Inicialmente vamos considerar equações da forma

$$a_1x_1 + \ldots + a_nx_n \equiv b \ (mod\, m) \tag{2.1}$$

onde $a_i \in \mathbb{Z}$, $i \in \{1,\ldots,n\}$, $b \in \mathbb{Z}$, $m \in \mathbb{Z}^*_+$(inteiros positivos).

Em primeiro lugar vamos considerar o caso especial em que $n = 1$, isto é,

$$ax \equiv b \ (mod\, m). \tag{2.2}$$

Para este caso, temos o seguinte resultado:

Teorema 2.1. *A equação* $ax \equiv b \ (mod\, m)$ $(a,b \in \mathbb{Z},\ m \in \mathbb{Z}^*_+)$ *tem solução se, e somente se,* $d|b$ *sendo* $d = mdc\,(a,m)$. *Neste caso, existem* d *soluções incongruentes módulo* m *que são*

$$x = x_0 + \frac{m}{d}r$$

onde $0 \leq r < d$ *e* x_0 *é uma solução qualquer da equação 2.2*

Prova. Note que investigar a existênca de soluções para a equação $ax \equiv b \ (mod\, m)$ é equivalente a investigar a existência de soluções para a equação

$$ax + my = b \tag{2.3}$$

pois,

$ax \equiv b \ (mod\, m) \Rightarrow \exists\, y^{'} \in \mathbb{Z}$ tal que $ax - b = my^{'} \Rightarrow ax - my^{'} = b \Rightarrow ax + m.(-y^{'}) = b.$
Tome $y = (-y^{'}) \in \mathbb{Z}$ e obtemos a equação (2.3).

Se a equação (2.3) tem solução em $\mathbb{Z}$, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + my_0 = b$. Como $d = mdc\,(a,m)$ $d|a$ e $d|m$, e portanto divide seus respectivos múltiplos, ou seja, $d|ax_0$ e $d|my_0$, logo concluímos que $d|(ax_0 + my_0)$ consequentemente $d|b$ como desejávamos.

Reciprocamente, consideremos $r, s \in \mathbb{Z}$, como $mdc\,(a,m) = d$ então pelo teorema 1.3 d é uma combinação linear de a e b

$$ar + ms = d. \tag{2.4}$$

Como temos por hipótese que $d|b$ então $b = dk$, com $k \in \mathbb{Z}$ e assim multiplicando (2.4) por k, teremos

$$b = dk = a(rk) + m(sk).$$

Tomando $x_0 = rk$ e $y_0 = sk$ temos $ax_0 + my_0 = b$, logo a equação (2.3) tem solução em $\mathbb{Z}$.

Agora precisamos encontrar a quantidade de soluções incongruentes módulo m, da equação (2.2).

Seja $x_0 \in \mathbb{Z}$ uma solução de (2.2). Vamos tentar mostrar inicialmente que todas as outras soluções são da forma

$$x = x_0 + \frac{m}{d}t, \quad \text{onde } t \in \mathbb{Z},$$

e depois mostraremos que dentre os valores de x, exatamente d são incongruentes módulo m.

Vamos então a existência das soluções.

Para $x = x_0 + \frac{m}{d}t$, multiplicamos a igualdade por a, temos

$$ax = ax_0 + \frac{am}{d}t = ax_0 + \left[\frac{at}{d}\right]m$$

e observe que a última igualdade da equação acima é da forma da equação (2.3). Mas, como estamos supondo que x_0 é solução da equação (2.2), consequentemente, é solução da equação (2.3), sendo assim, temos que $y_0 = \frac{at}{d} \in \mathbb{Z}$, também é solução de (2.3) uma vez que $d = mdc\,(a,m)$ e por isso $\frac{at}{d} \in \mathbb{Z}$,
logo,

$$ax \equiv ax_0 \ (mod\, m)$$

mas,

$$ax_0 \equiv b \ (mod\, m)$$

temos:

$$ax \equiv b \ (mod\, m)$$

assim, os números da forma $x = x_0 + \frac{m}{d}t$, $t \in \mathbb{Z}$ são soluções inteiras da equação (2.2).

Suponha agora que x é solução de (2.2). Então $ax \equiv b \ (mod\, m)$ e daí existe $y \in \mathbb{Z}$ talque $ax - b = ym$.

Como x_0 é solução de (2.2) existe $y_0 \in \mathbb{Z}$ talque $ax_0 - b = y_0 m$, portanto, da segunda das equações acima obtemos $-b = y_0 m - ax_0$ o que implica $b = ax_0 - y_0 m$. Tomando agora a primeira das equações e substituindo b, obtemos $ax - (ax_0 - y_0 m) = ym$, logo $(ax - ax_0) + y_0 m = ym$ donde segue que $a(x - x_0) = (y - y_0)m$. Como $d = mdc\,(a,m)$ temos que $a = a_1 d$ e $m = m_1 d$.

Observe que

$$a_1 d(x - x_0) = (y - y_0)m_1 d$$

cancelando o fator com d,

$$a_1(x - x_0) = (y - y_0)m_1$$

assim sendo, $m_1 | (a_1(x - x_0))$.

Observe ainda que o $mdc\,(a/d, b/d) = \frac{1}{d} \cdot mdc\,(a,b) = \frac{1}{d} \cdot d = 1$ e como $a_1 = \frac{a}{d}$ e $m_1 = \frac{m}{d}$ o $mdc\,(a_1, m_1) = 1$, logo, $m_1 | (x - x_0)$, isto é, existe $t \in \mathbb{Z}$ tal que $x - x_0 = m_1 t$ mas, por ser $m_1 = \frac{m}{d}$ temos: $x - x_0 = \frac{m}{d}t$ e finalmente, $x = x_0 + \frac{m}{d}t$.

Assim fica estabelecida a forma geral das soluções de (2.2). Dentre estas soluções é claro que

$$x_0, x_0 + \frac{m}{d}, x_0 + \frac{m}{d}2, \ldots, x_0 + \frac{m}{d}(d-1)$$

são incongruentes módulo m. Se agora $y = x_0 + \frac{m}{d}t$ é uma solução qualquer de (2.2), pelo algoritmo da divisão de Euclides temos $t = q.d + r$ com $q, r \in \mathbb{Z}$ e $0 \leq r < d$ e portanto

$$y = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(q.d + r) = x_0 + qm + r\frac{m}{d},$$

daí, $y \equiv x_0 + r \cdot \frac{m}{d} \ (mod\, m)$, logo existem exatamente d destas soluções que são incongruentes módulo m. ■

Corolário 2.1. *Se o $mdc\,(a,m) = 1$, então a congruência linear $ax \equiv b \ (mod\, m)$ tem uma única solução módulo* m.

Prova. Como o $mdc\,(a,m) = 1$ pelo teorema 1.3 existem inteiros r e s tais que

$$ar + ms = 1,$$

ou seja, 1 pode ser escrito como combinação linear de a e m. Multiplicando esta equação por b, temos

$$abr + mbs = b \Rightarrow a.(br) - b = m.(-bs)$$

tomando $x = br$ chegamos a equação

$$ax - b = m.(-bs)$$

ou

$$ax \equiv b \ (mod\, m).$$

Como vimos no teorema 2.1 as soluções para a equação (2.2) são da forma $x = x_0 + \frac{m}{d}t$, onde $t \in \mathbb{Z}$. Mas, para este caso, queremos provar que a equação (2.2) possui solução única módulo m. Com efeito, $x = x_0 + m.t$ é solução da equação $ax \equiv b \ (mod\, m)$, logo, as demais soluções da equação são devidas aos valores de t. Assim, por ser $1 = mdc\,(a,m)$ temos, pelo mesmo teorema, que $0 \leq t < 1$ e como $t \in \mathbb{Z}$ então $t = 0$. Portanto $x = x_0$ é a única solução incongruente módulo m da equação enunciada. ■

Exemplo 2.1. *Resolver a congruência linear* $3x \equiv 1 \ (mod\, 5)$.

Solução: Como o $mdc(3,5) = 1$, e 1 divide 1, pelo corolário 2.1 a congruência linear $3x \equiv 1(mod\, 5)$, possui uma única solução. Vamos agora determinar essa solução.

Como,

$$3x \equiv 1(mod\, 5) \Longleftrightarrow 5|(3x-1) \Longleftrightarrow \exists\, y_0 \in \mathbb{Z}; 3x - 1 = 5y_0 \Longleftrightarrow 3x - 5y_0 = 1.$$

Portanto, para resolver a congruência linear $3x \equiv 1(mod\, 5)$, basta resolver a equação diofantina

$$3x - 5y_0 = 1.$$

Pelo algoritmo de Euclides, temos que:

$$\begin{aligned} 5 &= 3.1 + 2 \\ 3 &= 2.1 + 1 \\ 2 &= 1.2 + 0. \end{aligned}$$

Donde se deduz que

$$1 = 3 - 2.1 = 3 - (5 - 3.1).1 = 3 - 5 + 3 = 3.2 - 5$$

isto é, o par de inteiros $x_0 = 2$ e $y_0 = 1$ é uma solução da equação diofantina linear

$$3x - 5y_0 = 1$$

e, portanto, $x_0 = 2$ é uma solução da congruência linear $3x \equiv 1(mod\,5)$. Logo, as demais soluções desta equação é da forma $x = 2 + 5t$, onde $t \in \mathbb{Z}$.

Exemplo 2.2. *Encontre as soluções da congruência linear* $21x \equiv 9\ (mod\,15)$, *caso existam.*

Solução: Como o $mdc(21, 9) = 3$, e 3 divide 15, pelo teorema 2.1 a congruência linear $21x \equiv 9\ (mod\,15)$, possui três soluções incongruentes. Vamos agora determinar essas soluções.

Como,

$$21x \equiv 9\ (mod\,15) \Longleftrightarrow 15|(21x-9) \Longleftrightarrow \exists\, y \in \mathbb{Z}; 21x-9 = 15y \Longleftrightarrow 21x-15y = 9.$$

Portanto, para resolver a congruência linear $21x \equiv 9\ (mod\,15)$, basta resolver a equação diofantina

$$21x - 15y = 9.$$

Pelo algoritmo de Euclides, temos que:

$$\begin{array}{rcrcr} 21 & = & 15.1 & + & 6 \\ 15 & = & 6.2 & + & 3 \\ 6 & = & 3.2 & + & 0. \end{array}$$

Como já sabemos, o $mdc(21,15) = 3$. Assim como no teorema 1.3, vamos escrever 3 como combinação linear de 21 e 15. Logo, pelo algoritmo de Euclides, se deduz que

$$3 = 15 - 6\cdot(2) = 15 - (21-15)\cdot(2) = 15 - 21\cdot(2) + 15\cdot(2) = 15\cdot(3) - 21\cdot(2)$$

ou seja, $3 = 15(3) - 21(2)$, multiplicando esta equação por 3, obtemos,

$$9 = 15\cdot(9) - 21\cdot(6)$$

que não está da forma $21x - 15y = 9$. Assim, fazendo

$$9 = 21\cdot(-6) - 15\cdot(-9)$$

obtemos o par de inteiros $x_0 = -6$ e $y_0 = -9$ que é uma solução da equação diofantina linear

$$21x - 15y_0 = 9$$

e, portanto, $x_0 = -6$ é uma solução da congruência linear $21x \equiv 9\ (mod\,15)$. Logo, as demais soluções desta equação são da forma $x = -6 + 5t$, onde $t \in \mathbb{Z}$.

Exemplo 2.3. *Resolver a congruência linear* $35x \equiv 5\ (mod\,14)$.

Solução: O $mdc\,(35,14) = 7$ e como 7 não divide 5, a congruência linear dada não tem solução.

Inverso de um inteiro

Definição 2.1. *Seja a um inteiro. Denominamos inverso de a módulo* m *um inteiro* a^* *tal que* $aa^* \equiv 1 \ (mod\, m)$.

Teorema 2.2. *Seja o* $mdc\,(a, m) = 1$, *então a tem um único inverso módulo m.*

Prova. Considere a congruência linear $ax \equiv 1 \ (mod\, m)$, se o $mdc\,(a, m) = 1$ então a congruência admite uma única solução $x_0 \ (mod\, m)$, isto é, $ax_0 \equiv 1 \ (mod\, m)$ de modo que o inteiro a tem um único inverso módulo m: $a^* = x_0$. ■

Exemplo 2.4. *Por ser* $3 \cdot 3 \equiv 1 \ (mod\, 4)$, *segue-se que o inverso de* 3 *módulo* 4 *é o próprio* 3. *Observe também que* $3 \cdot 7 \equiv 1 \ (mod\, 4)$ *e* $3 \cdot (-1) \equiv 1 \ (mod\, 4)$ *de modo que* 7 *e* -1 *são, respectivamente, inversos de 3 módulo 4, mas, segundo o teorema 2.2 como o inverso de um inteiro se existir é único, temos que*

$$-1 \equiv 3 \equiv 7 \ (mod\, 4).$$

Exemplo 2.5. *O inverso de* $2a^* \equiv 1 \ (mod\, 5)$ *é* $a^* = 3$, *pois, de acordo com o teorema 2.2, o inverso de* 2 *existe, por que, o* $mdc\,(2, 5) = 1$ *e é único.*

Exemplo 2.6. $3a^* \equiv 1 \ (mod\, 9)$ *não admite inverso módulo* 9, *pois, para existir, o* $mdc(3, 9)$ *teria que ser* 1. *E neste caso, o* $mdc\,(3, 9) = 3$.

Agora vamos voltar ao caso geral da equação 2.1 qual seja,

$$a_1x_1 + \ldots + a_nx_n \equiv b \ (mod\, m), \quad \text{com } n \geq 1.$$

O seguinte teorema determina as condições para existência de soluções para esta equação:

Teorema 2.3. *A condição necessária e suficiente para que a equação 2.1*

$$a_1x_1 + \ldots + a_nx_n \equiv b \ (mod\, m)$$

tenha solução é que $d|b$, *onde* $d = mdc\,(a_1, \ldots, a_n, m)$.

Prova. Esta demonstração generaliza as idéias apresentadas na primeira parte da demonstração do Teorema 2.1 (referente a existência de soluções da equação 2.2). Vamos observar inicialmente que a condição é necessária. Com efeito, dizer que 2.1 tem solução é dizer que existem $x_1, \ldots, x_n, y$ em $\mathbb{Z}$ tais que

$$a_1x_1 + \ldots + a_nx_n - b = ym$$

o que implica

$$-b = -(a_1x_1 + \ldots + a_nx_n) + ym$$

ou,

$$b = a_1x_1 + \ldots + a_nx_n - ym$$

e daí vemos que $d = mdc\,(a_1, \ldots, a_n, m)$ divide b.

Vamos agora investigar a suficiência da condição citada. O que faremos é reduzir o problema para o caso $n = 1$ (já estudado).

Seja o $mdc\,(a_1, \ldots, a_{n-1}, m) = d_1$. Então, temos que

(I) Existem $r_1, \ldots, r_{n-1}, s$ em $\mathbb{Z}$ tais que $r_1a_1 + \ldots + r_{n-1}a_{n-1} + sm = d_1$.

(II) $mdc(a_n, d_1) = d$.

Da condição (II), usando o teorema 2.1, obtemos que a equação $a_nx_n \equiv b\ (mod\, d_1)$ tem solução, pois, o $(mdc(a_n, d_1) = d$ e $d|b)$, isto é, existem x_n e t em $\mathbb{Z}$ tais que

$$a_nx_n - td_1 = b. \tag{2.5}$$

Veja que, $a_nx_n \equiv b\ (mod\, d_1) \Rightarrow \exists t \in \mathbb{Z}$ tal que $a_nx_n - b = td_1 \Rightarrow a_nx_n - td_1 = b$.

Utilizando (I) em (2.5) obtemos:

$$a_nx_n - t(r_1a_1 + \ldots + r_{n-1}a_{n-1} + sm) = b$$

daí,

$$a_nx_n - tr_1a_1 - \ldots - tr_{n-1}a_{n-1} - tsm = b$$

ou,

$$a_1(-tr_1) + \ldots + a_{n-1}(-tr_{n-1}) + a_nx_n + m(-ts) = b$$

o que implica

$$a_1(-tr_1) + \ldots + a_{n-1}(-tr_{n-1}) + a_nx_n - b = (ts)m,$$

ou seja, $x_1 = -tr_1$, ..., $x_{n-1} = -tr_{n-1}$ e o x_n encontrado antes satisfazem

$$a_1x_1 + \ldots + a_nx_n \equiv b\ (mod\, m)$$

como desejávamos. ■

Vamos fixar as idéias através de exemplos.

Exemplo 2.7. *Obtenha uma solução da equação* $4x + 7y \equiv 5\ (mod\, 14)$.

Solução: Pela definição de congruência $14|\,[(4x + 7y) - 5] \Rightarrow \exists z \in \mathbb{Z}$ tal que $4x + 7y - 14z = 5$ e o $mdc\,(4, 7, 14) = 1$, como 1 divide qualquer inteiro, concluímos que a equação admite uma solução. Seguindo a demonstração do teorema 2.3, temos $d_1 = (4, 14) = 2$ e podemos escrever como combinação linear de inteiros

$$2 = 4(4) - 14(1). \tag{2.6}$$

Agora $mdc\,(7,2)=1$ e então podemos escrever 1 como uma combinação linear de inteiros. Veja,

$$1=7(1)-2(3)$$

multiplicando ambos os membros da equação acima por 5, obtemos

$$5=7(5)-2(15). \tag{2.7}$$

substituindo então a expressão (2.6) na expressão (2.7) e chegamos a

$$5=7(5)-(4(4)-14(1))\,15=7(5)+(4(-4)+14(1))\,15=4(-60)+7(5)+14(15).$$

Portanto, $x=-60$ e $y=5$ são soluções da equação de congruência acima.

Exemplo 2.8. *Resolva a equação* $3x+9y+11z\equiv 9\ (mod\,13)$.

Solução: Inicialmente, pela definição 1.7 podemos escrever a congruência linear acima, como uma equação da forma

$$3x+9y+11z-9=13t,\ \text{com}\ t\in\mathbb{Z},$$

ou ainda,

$$3x+9y+11z-13t=9.$$

Como $d=mdc\,(3,9,11,13)=1$, a equação admite uma solução. Daí, temos $d_1=mdc\,(3,9,13)=$ 1e podemos escrever

$$1=3.(15)-9.(2)-13.(2). \tag{2.8}$$

Agora $mdc\,(11,1)=1$ e então podemos escrever 1 como combinação linear dos inteiros 11 e 1

$$1=11.(1)-1.(10),$$

multiplicando por 9, obtemos:

$$9=11.(9)-1.(90). \tag{2.9}$$

Substituindo a equação (2.8) na equação (2.9) chegamos ao seguinte resultado:

$$9=11.(9)-(3.(15)-9.(2)-13.(2))\,.90=11.(9)+3.(-1350)+9.(180)+13.(180)=$$

$$=3.(-1350)+9.(180)+11.(9)+13.(180).$$

Portanto, $x=-1350$, $y=180$ e $z=9$ são soluções da equação de congruência acima.

Observe que no Teorema 2.3 bem como nos exemplos supracitados, estavámos preocupados apenas com a existência de soluções para uma equação de congruência do tipo (2.1). Agora queremos investigar a quantidade de soluções incongruentes módulo m da equação (2.1), no caso em que, esta admitir solução. Sendo assim, $(x_1,\ldots,x_n)$ e $(y_1,\ldots,y_n)$ são duas soluções incongrentes módulo m de (2.1) se existe $j\in\{1,2,\ldots,n\}$ tal que $x_j\not\equiv y_j\ (mod\,m)$.

Lema 2.1. *Seja* $m \in \mathbb{Z}_+^*$, $a_1, \ldots, a_n, b \in \mathbb{Z}$ *e* $d = (a_1, \ldots, a_n, m)$. *Suponha que* $d|b$. *Então a equação de congruência*

$$a_1x_1 + \ldots + a_nx_n \equiv b \ (mod\, m) \tag{2.10}$$

admite dm^{n-1} *soluções incongruentes módulo* m.

Prova. Faremos a demonstração por indução sobre n.

Se $n = 1$, temos $d = mdc\,(a_1, m)$ e por hipótese $d|b$, então o Teorema 2.1 nos diz que existem d soluções da equação $a_1x_1 \equiv b \ (mod\, m)$ que são incongruentes módulo m. Portanto, no caso $n = 1$ a afirmação é verdadeira.

Suponha agora que temos $n > 1$ e seja

$$d_1 = mdc\,(a_1, \ldots, a_{n-1}, m).$$

O argumento indutivo desenvolvido aqui baseia-se no fato de que se a equação acima admite uma solução $(x_1, \ldots, x_n)$ então, necessariamente, devemos ter

$$a_1x_1 + \ldots + a_{n-1}x_{n-1} + a_nx_n - a_nx_n \equiv b - a_nx_n \ (mod\, m)$$

ou seja,

$$a_1x_1 + \ldots + a_{n-1}x_{n-1} \equiv b - a_nx_n \ (mod\, m).$$

Observe que d_1 divide a_i, $i \in \{1, \ldots, n-1\}$, logo divide $a_1x_1 + \ldots + a_{n-1}x_{n-1}$ e isto implica que d_1 divide $b - a_nx_n$, ou seja, $a_nx_n \equiv b \ (mod\, d_1)$. Devemos lembrar que a variável x_n pode assumir qualquer valor no conjunto $\{0, 1, 2, \ldots, m-1\}$ pois a equação original possui módulo m.

De acordo com a definição da condição (II) temos que $d = mdc\,(a_n, d_1)$, portanto a equação $a_nx_n \equiv b \ (mod\, d_1)$ tem exatamente d soluções incongruentes, $x_n^{(1)}, \ldots, x_n^{(d)}$,módulo d_1. Vamos escolher estas soluções de tal modo que $0 \leq x_n^{(j)} < d_1$, $j \in \{1, \ldots, d\}$. Para cada $j \in \{1, \ldots, d\}$ construímos o conjunto

$$X_j = \left\{ y = x_n^{(j)} + kd_1 : k = 0, 1, \ldots, (\frac{m}{d_1} - 1) \right\}.$$

Agora fixe $j \in \{1, \ldots, d\}$ e escolha $y \in X_j$. Este elemento y possui as seguintes propriedades

(I) $a_nx_n = a_ny = a_n(x_n^{(j)} + kd_1) = a_nx_n^{(j)} + a_nkd_1 \equiv a_nx_n^{(j)} \equiv b \ (mod\, d_1)$, pois $x_n^{(j)}$ é solução de $a_nx_n \equiv b \ (mod\, d_1)$.

(II) $0 \leq y = x_n^{(j)} + kd_1 \leq x_n^{(j)} + \left(d\frac{m}{d_1} - 1\right) d_1 = x_n^{(j)} + m - d_1 < m$, pois, $0 \leq x_n^{(j)} < d_1$. Assim, em cada conjunto X_j, $j \in \{1, \ldots, d\}$ existem $\frac{m}{d_1}$ inteiros y tais que

$$0 \leq y < m \text{ e } a_ny \equiv b \ (mod\, d_1).$$

Como temos d conjuntos X_j, no total teremos $\frac{md}{d_1}$ inteiros y distintos tais que $0 \leq y < m$ e $a_n y \equiv b \,(mod\, d_1)$. Substituindo cada um desses inteiros na equação

$$a_1x_1 + \ldots + a_{n-1}x_{n-1} + a_nx_n \equiv b \,(mod\, m)$$

(no lugar do x_n, claro!) obtemos $\frac{md}{d_1}$ equações do tipo

$$a_1x_1 + \ldots + a_{n-1}x_{n-1} \equiv (b - a_ny) \,(mod\, m).$$

A propriedade (I) anterior nos diz que $d_1|(b - a_ny)$ (pois (I) nos fornece $b - a_ny \equiv 0 \,(mod\, d_1)$, onde $d_1 = (a_1, \ldots, a_{n-1}, m)$, portanto, cada equação acima está nas mesmas condições da equação original mas, com $n-1$ variáveis. Por hipótese de indução, cada uma destas equações admite d_1m^{n-2} soluções incongruentes módulo m. Como são $\frac{md}{d_1}$ equações, vemos que a equação de congruência original admite $d_1m^{n-2}.\frac{md}{d_1} = dm^{n-1}$ soluções incongruentes módulo m. ■

A seguir iremos determinar a quantidade de soluções de cada uma das equações abaixo.

Exemplo 2.9. *Determinar todas as soluções da equação* $4x + 7y = 5 \,(mod\, 14)$.

Solução: Como $d = mdc(4, 7, 14) = 1$, $m = 14$ e $n = 2$, concluímos que esta equação possui $dm^{n-1} = 1.14^1 = 14$ soluções incongruentes.

Seja $d_1 = mdc\,(4, 14) = 2$, e observe que a equação $7y \equiv 5 \,(mod\, 2)$ admite uma única solução $y = 1$ (pois $d = mdc\,(a_n, d_1) = (7, 2) = 1$).

De acordo com a definição, $x_n^{(1)} = 1$ é a única solução incongruente encontrada e como $d = 1$ formamos apenas um conjunto X_1, com os seguintes elementos logo,

$$X_1 = \{1, 3, 5, 7, 9, 11, 13\}.$$

Considere agora as congruências

(i) $4x + 7.1 \equiv 5 \,(mod\, 14)$
(ii) $4x + 7.3 \equiv 5 \,(mod\, 14)$
(iii) $4x + 7.5 \equiv 5 \,(mod\, 14)$
(iv) $4x + 7.7 \equiv 5 \,(mod\, 14)$
(v) $4x + 7.9 \equiv 5 \,(mod\, 14)$
(vi) $4x + 7.11 \equiv 5 \,(mod\, 14)$
(vii) $4x + 7.13 \equiv 5 \,(mod\, 14)$

(i) $4x \equiv 5 - 7 \,(mod\, 14)$
(ii) $4x \equiv 5 - 21 \,(mod\, 14)$
(iii) $4x \equiv 5 - 35 \,(mod\, 14)$
(iv) $4x \equiv 5 - 49 \,(mod\, 14)$

(v) $4x \equiv 5-63\ (mod\,14)$
(vi) $4x \equiv 5-77\ (mod\,14)$
(vii) $4x \equiv 5-91\ (mod\,14)$

que, como podemos observar, são todas equivalentes à equação

$$4x \equiv -2\ (mod\,14).$$

Fazendo uso do teorema 2.1 verificamos que o $mdc\,(4,\,14) = 2$ e $2|-2$, logo as soluções das equações acima são $x = 3$ ou $x = 3 + \frac{14}{2}1 = 10$. Portanto, as soluções incongruentes da equação

$$4x + 7y \equiv 5\ (mod\,14)$$

são

{(3, 1), (10, 1), (3, 3), (10, 3), (3, 5), (10, 5), (3, 7), (10, 7), (3, 9), (10, 9), (3, 11), (10, 11), (3, 13), (10, 13)}

Exemplo 2.10. *Ache o número de soluções da equação de congruência* $5x + 25y + 50z \equiv 15\ (mod\,10)$.

Solução: O $d = mdc\,(5, 25, 50, 10) = 5$, $m = 10$ e $n = 3$, assim, a equação admite $5.10^{3-1} = 5.10^2 = 500$ soluções incongruentes.

Seja $d_1 = mdc\,(5, 25, 10) = 5$, e observe que a equação $50z \equiv 15\ (mod\,5)$ admite cinco soluções incongruentes módulo 5 (pois $d = mdc\,(a_n, d_1) = mdc\,(50, 5) = 5$ e $5|15$). Sendo assim, utilizaremos $z = 0 + \frac{5}{5}t = 0 + 1.t$, com $t = 0, 1, 2, 3, 4$ para encontrarmos tais soluções, quais sejam

$$z_1 = 0, \qquad z_2 = 1, \qquad z_3 = 2, \qquad z_4 = 3 \qquad \text{e} \qquad z_5 = 4.$$

Para cada solução construímos os conjuntos X_j logo,

$$X_1 = \{0, 5\}, \quad X_2 = \{1, 6\}, \quad X_3 = \{2, 7\}, \quad X_4 = \{3, 8\} \quad \text{e} \quad X_5 = \{4, 9\},$$

observe que em cada conjunto acima existem 2 inteiros y tais que $0 \leq y < 10$ e como temos 5 conjuntos, no total teremos $\frac{10.5}{5} = 10$ inteiros y distintos tais que $0 \leq y < 10$ e satisfazem a congruência $50z \equiv 15\ (mod\,5)$.

Considere agora as congruências

$$
\begin{aligned}
&(i)\ 5x+25y+50.0 \equiv 15\ (mod\,10)\\
&(ii)\ 5x+25y+50.1 \equiv 15\ (mod\,10\\
&(iii)\ 5x+25y+50.2 \equiv 15\ (mod\,10)\\
&(iv)\ 5x+25y+50.3 \equiv 15\ (mod\,10)\\
&(v)\ 5x+25y+50.4 \equiv 15\ (mod\,10)\\
&(vi)\ 5x+25y+50.5 \equiv 15\ (mod\,10)\\
&(vii)\ 5x+25y+50.6 \equiv 15\ (mod\,10)\\
&(viii)\ 5x+25y+50.7 \equiv 15\ (mod\,10)\\
&(ix)\ 5x+25y+50.8 \equiv 15\ (mod\,10)\\
&(x)\ 5x+25y+50.9 \equiv 15\ (mod\,10).
\end{aligned}
$$

e observe que são todas equivalentes à equação

$$5x+25y \equiv 15\ (mod\,10). \tag{2.11}$$

Como já vimos anteriormente, teremos que fazer o procedimento análogo à z.

Repare que $25y \equiv 15\ (mod\,5)$ então podemos afirmar, que esta equação possui exatamente cinco soluções incongruentes módulo 5. Logo, obtemos os 5 conjuntos X_j

$$X_1=\{0,5\},\quad X_2=\{1,6\},\quad X_3=\{2,7\},\quad X_4=\{3,8\}\quad \text{e}\quad X_5=\{4,9\}.$$

Considere as congruências

$$
\begin{aligned}
&(i^{'})\ 5x+25.0 \equiv 15\ (mod\,10)\\
&(ii^{'})\ 5x+25.1 \equiv 15\ (mod\,10)\\
&(iii^{'})\ 5x+25.2 \equiv 15\ (mod\,10)\\
&(iv^{'})\ 5x+25.3 \equiv 15\ (mod\,10)\\
&(v^{'})\ 5x+25.4 \equiv 15\ (mod\,10)\\
&(vi^{'})\ 5x+25.5 \equiv 15\ (mod\,10)\\
&(vii^{'})\ 5x+25.6 \equiv 15\ (mod\,10)\\
&(viii^{'})\ 5x+25.7 \equiv 15\ (mod\,10)
\end{aligned}
$$

$$
\begin{aligned}
&(ix^{'})\ 5x+25.8 \equiv 15\ (mod\,10)\\
&(x^{'})\ 5x+25.9 \equiv 15\ (mod\,10),
\end{aligned}
$$

como podemos concluir, $i^{'}$, $iii^{'}$, $v^{'}$, $vii^{'}$, $ix^{'}$ são equivalentes à

$$5x \equiv 15\ (mod\,10) \tag{2.12}$$

e ii', iv', vi', $viii'$, x' são equivalentes à

$$5x \equiv -10 \ (mod\, 10) \tag{2.13}$$

daí, observamos que (2.12) e (2.13) possuem, cada qual respectivamente, cinco soluções incongruentes módulo 10.

$$x = 1, 3, 5, 7, 9$$

e

$$x = 0, 2, 4, 6, 8.$$

Como a equação 2.12 é equivalente a cinco das dez equações acima e a equação 2.13 é equivalente as demais, no total temos 50 soluções incongruentes para a equação 2.11 e como esta, por sua vez, é equivalente as equações $i, ii, \ldots, x$, temos que, cada uma admite 50 soluções distintas em módulo. Assim, contabilizamos 500 soluções incongruentes para a equação

$$5x + 25y + 50z \equiv 15 \ (mod\, 10).$$

São elas:
{(1, 0, 0), (1, 0, 1), (1, 0, 2), (1, 0, 3), (1, 0, 4), (1, 0,5), (1, 0, 6), (1, 0, 7), (1, 0, 8), (1, 0, 9), (1, 2, 0), (1, 2, 1), (1, 2, 2), (1, 2, 3), (1, 2, 4), (1, 2, 5), (1, 2, 6), (1, 2, 7), (1, 2, 8), (1, 2, 9), (1, 4, 0), (1, 4, 1), (1, 4, 2), (1, 4, 3), (1, 4, 4), (1, 4, 5), (1, 4, 6), (1, 4, 7), (1, 4, 8), (1, 4, 9), (1, 6, 0), (1, 6, 1), (1, 6, 2), (1, 6, 3), (1, 6, 4), (1, 6, 5), (1, 6, 6), (1, 6, 7), (1, 6, 8), (1, 6, 9), (1, 8, 0), (1, 8, 1), (1, 8, 2), (1, 8, 3), (1, 8, 4), (1, 8, 5), (1, 8, 6), (1, 8, 7), (1, 8, 8), (1, 8, 9), (3, 0, 0), (3, 0, 1), (3, 0, 2), (3, 0, 3), (3, 0, 4), (3, 0, 5), (3, 0, 6), (3, 0, 7), (3, 0, 8), (3, 0, 9), (3, 2, 0), (3, 2, 1), (3, 2, 2), (3, 2, 3), (3, 2, 4), (3, 2, 5), (3, 2, 6), (3, 2, 7), (3, 2, 8), (3, 2, 9), (3, 4, 0), (3, 4, 1), (3, 4, 2), (3, 4, 3), (3, 4, 4), (3, 4, 5), (3, 4, 6), (3, 4, 7), (3, 4, 8), (3, 4, 9), (3, 6, 0), (3, 6, 1), (3, 6, 2), (3, 6, 3), (3, 6, 4), (3, 6, 5), (3, 6, 6), (3, 6, 7), (3, 6, 8), (3, 6, 9), (3, 8, 0), (3, 8, 1), (3, 8, 2), (3, 8, 3), (3, 8, 4), (3, 8, 5), (3, 8, 6), (3, 8, 7), (3, 8, 8), (3, 8, 9), (5, 0, 0), (5, 0, 1), (5, 0, 2), (5, 0, 3), (5, 0, 4), (5, 0, 5), (5, 0, 6), (5, 0, 7), (5, 0, 8), (5, 0, 9), (5, 2, 0), (5, 2, 1), (5, 2, 2), (5, 2, 3), (5, 2, 4), (5, 2, 5), (5, 2, 6), (5, 2, 7), (5, 2, 8), (5, 2, 9), (5, 4, 0), (5, 4, 1), (5, 4, 2), (5, 4, 3), (5, 4, 4), (5, 4, 5), (5, 4, 6), (5, 4, 7), (5, 4, 8), (5, 4, 9), (5, 6, 0), (5, 6, 1), (5, 6, 2), (5, 6, 3), (5, 6, 4), (5, 6, 5), (5, 6, 6), (5, 6, 7), (5, 6, 8), (5, 6, 9), (5, 8, 0), (5, 8, 1), (5, 8, 2), (5, 8, 3), (5, 8, 4), (5, 8, 5), (5, 8, 6), (5, 8, 7), (5, 8, 8), (5, 8, 9), (7, 0 , 0), (7, 0, 1), (7, 0, 2), (7, 0, 3), (7, 0, 4), (7, 0, 5), (7, 0, 6), (7, 0, 7), (7, 0, 8), (7, 0, 9), (7, 2, 0), (7, 2, 1), (7, 2, 2), (7, 2, 3), (7, 2, 4), (7, 2, 5), (7, 2, 6), (7, 2, 7), (7, 2, 8), (7, 2, 9), (7, 4, 0), (7, 4, 1), (7, 4, 2), (7, 4, 3), (7, 4, 4), (7, 4, 5), (7, 4, 6), (7, 4, 7), (7, 4, 8), (7, 4, 9), (7, 6, 0), (7, 6, 1), (7, 6, 2), (7, 6, 3), (7, 6, 4), (7, 6, 5), (7, 6, 6), (7, 6, 7), (7, 6, 8), (7, 6, 9), (7, 8, 0), (7, 8, 1), (7, 8, 2), (7, 8, 3), (7, 8, 4), (7, 8, 5), (7, 8, 6), (7, 8, 7), (7, 8, 8), (7, 8, 9), (9, 0, 0), (9, 0, 1), (9, 0, 2), (9, 0, 3), (9, 0, 4), (9, 0, 5), (9, 0, 6), (9, 0, 7), (9, 0, 8), (9, 0, 9), (9, 2, 0), (9, 2, 1), (9, 2, 2), (9, 2, 3), (9, 2, 4), (9, 2, 5), (9, 2, 6), (9, 2, 7), (9, 2, 8), (9, 2, 9), (9, 4, 0), (9, 4, 1), (9, 4, 2), (9, 4, 3), (9, 4, 4), (9, 4, 5), (9, 4, 6), (9,

4, 7), (9, 4, 8), (9, 4, 9), (9, 6, 0), (9, 6, 1), (9, 6, 2), (9, 6, 3), (9, 6, 4), (9, 6, 5), (9, 6, 6), (9, 6, 7), (9, 6, 8), (9, 6, 9), (9, 8, 0), (9, 8, 1), (9, 8, 2), (9, 8, 3), (9, 8, 4), (9, 8, 5), (9, 8, 6), (9, 8, 7), (9, 8, 8), (9, 8, 9), (0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 1, 3), (0, 1, 4), (0, 1, 5), (0, 1, 6), (0, 1, 7), (0, 1, 8), (0, 1, 9), (0, 3, 0), (0, 3, 1), (0, 3, 2), (0, 3, 3), (0, 3, 4), (0, 3, 5), (0, 3, 6), (0, 3, 7), (0, 3, 8), (0, 3, 9), (0, 5, 0), (0, 5, 1), (0, 5, 2), (0, 5, 3), (0, 5, 4), (0, 5, 5), (0, 5, 6), (0, 5, 7), (0, 5, 8), (0, 5, 9), (0, 7, 0), (0, 7, 1), (0, 7, 2), (0, 7, 3), (0, 7, 4), (0, 7, 5), (0, 7, 6), (0, 7, 7), (0, 7, 8), (0, 7, 9), (0, 9, 0), (0, 9, 1), (0, 9, 2), (0, 9, 3), (0, 9, 4), (0, 9, 5), (0, 9, 6), (0, 9, 7), (0, 9, 8), (0, 9, 9), (2, 1, 0), (2, 1, 1), (2, 1, 2), (2, 1, 3), (2, 1, 4), (2, 1, 5), (2, 1, 6), (2, 1, 7), (2, 1, 8), (2, 1, 9), (2, 3, 0), (2, 3, 1), (2, 3, 2), (2, 3, 3), (2, 3, 4), (2, 3, 5), (2, 3, 6), (2, 3, 7), (2, 3, 8), (2, 3, 9), (2, 5, 0), (2, 5, 1), (2, 5, 2), (2, 5, 3), (2, 5, 4), (2, 5, 5), (2, 5, 6), (2, 5, 7), (2, 5, 8), (2, 5, 9), (2, 7, 0), (2, 7, 1), (2, 7, 2), (2, 7, 3), (2, 7, 4), (2, 7, 5), (2, 7, 6), (2, 7, 7), (2, 7, 8), (2, 7, 9), (2, 9, 0), (2, 9, 1), (2, 9, 2), (2, 9, 3), (2, 9, 4), (2, 9, 5), (2, 9, 6), (2, 9, 7), (2, 9, 8), (2, 9, 9), (4, 1, 0), (4, 1, 1), (4, 1, 2), (4, 1, 3), (4, 1, 4), (4, 1, 5), (4, 1, 6), (4, 1, 7), (4, 1, 8), (4, 1, 9), (4, 3, 0), (4, 3, 1), (4, 3, 2), (4, 3, 3), (4, 3, 4), (4, 3, 5), (4, 3, 6), (4, 3, 7), (4, 3, 8), (4, 3, 9), (4, 5, 0), (4, 5, 1), (4, 5, 2), (4, 5, 3), (4, 5, 4), (4, 5, 5), (4, 5, 6), (4, 5, 7), (4, 5, 8), (4, 5, 9), (4, 7, 0), (4, 7, 1), (4, 7, 2), (4, 7, 3), (4, 7, 4), (4, 7, 5), (4, 7, 6), (4, 7, 7), (4, 7, 8), (4, 7, 9), (4, 9, 0), (4, 9, 1), (4, 9, 2), (4, 9, 3), (4, 9, 4), (4, 9, 5), (4, 9, 6), (4, 9, 7), (4, 9, 8), (4, 9, 9), (6, 1, 0), (6, 1, 1), (6, 1, 2), (6, 1, 3), (6, 1, 4), (6, 1, 5), (6, 1, 6), (6, 1, 7), (6, 1, 8), (6, 1, 9), (6, 3, 0), (6, 3, 1), (6, 3, 2), (6, 3, 3), (6, 3, 4), (6, 3, 5), (6, 3, 6), (6, 3, 7), (6, 3, 8), (6, 3, 9), (6, 5, 0), (6, 5, 1), (6, 5, 2), (6, 5, 3), (6, 5, 4), (6, 5, 5), (6, 5, 6), (6, 5, 7), (6, 5, 8), (6, 5, 9), (6 , 7, 0), (6, 7, 1), (6, 7, 2), (6, 7, 3), (6, 7, 4), (6, 7, 5), (6, 7, 6), (6, 7, 7), (6, 7, 8), (6, 7, 9), (6, 9, 0), (6, 9, 1), (6, 9, 2), (6, 9, 3), (6, 9, 4), (6, 9, 5), (6, 9, 6), (6, 9, 7), (6, 9, 8), (6, 9, 9), (8,1, 0), (8, 1, 1), (8,1, 2), (8, 1, 3), (8, 1, 4), (8, 1, 5), (8, 1, 6), (8, 1, 7), (8, 1, 8), (8, 1, 9), (8, 3, 0), (8, 3, 1), (8, 3, 2), (8, 3, 3), (8, 3, 4), (8, 3, 5), (8, 3, 6), (8, 3, 7), (8, 3, 8), (8, 3, 9), (8, 5, 0), (8, 5, 1), (8, 5, 2), (8, 5, 3), (8, 5, 4), (8, 5, 5), (8, 5, 6), (8, 5, 7), (8, 5, 8), (8, 5, 9), (8, 7, 0), (8, 7, 1), (8, 7, 2), (8, 7, 3), (8, 7, 4), (8, 7, 5), (8, 7, 6), (8, 7, 7), (8, 7, 8), (8, 7, 9), (8, 9, 0), (8, 9, 1), (8, 9, 2), (8, 9, 3), (8, 9, 4), (8, 9, 5), (8, 9, 6), (8, 9, 7), (8, 9, 8), (8, 9, 9)}

Observe então que a demonstração deste lema nos fornece um processo algorítmico para chegar às soluções da equação de congruência dada.

2.2 Sistemas de Equações de Grau Um

Nesta seção lidaremos com a resolução de sistemas de equações de congruência, que resumem-se ao problema de encontrar solução para várias equações ao mesmo tempo.

Inicialmente consideraremos equações do tipo

$$x \equiv c_j \ (mod\, m_j)$$

para $c_j \in \mathbb{Z}$, $m_j \in \mathbb{Z}_+^*$ e $j \in \{1, 2, \ldots, n\}$, $n \in \mathbb{N}$. Assim resolvemos adotar, por ser mais didático e de melhor compreensão, primeiramente, casos particulares como o Teorema do Resto Chinês e depois, um resultado mais geral que resolve completamente o nosso problema.

Teorema 2.4. *(***Teorema Chinês do Resto***) Sejam* $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ *e* $m_1, m_2, \ldots m_k \in \mathbb{N}$ *tais que* $mdc(m_i, m_j) = 1$, *com* $i \neq j$. *Então o sistema de congruências*

$$\begin{cases} x & \equiv & a_1 (mod.m_1) \\ x & \equiv & a_2 (mod.m_2) \\ x & \equiv & a_3 (mod.m_3) \\ \vdots & & \\ x & \equiv & a_k (mod.m_k) \end{cases} \tag{2.14}$$

tem uma única solução x_0 *com* $1 \leq x_0 < m$, *onde* $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$. *Além disso,*

$$S = \{x_0 + km : k \in \mathbb{Z}\}$$

é o conjunto de todas as soluções do sistema 2.14.

Prova. Para cada $r = 1, 2, \ldots, k$, seja:

$$M_r = \frac{m}{m_r} = m_1 \cdot m_2 \cdot \ldots \cdot m_{r-1} \cdot m_{r-2} \cdot \ldots m_k$$

Assim,

$$mdc(\frac{m}{m_r}, m_r) = mdc(M_r, m_r) = 1$$

e, portanto, pelo teorema 2.2

$$M_r x \equiv 1 (mod.m_r) \tag{2.15}$$

tem solução única, vamos denotar esta solução por x_r.

Portanto, vamos demonstrar que o inteiro:

$$X = a_1 M_1 x_1 + a_2 M_2 x_2 + \ldots + a_k M_k x_k$$

satisfaz cada uma das congruências do sistema 2.14 considerado, ou seja, que X é uma solução deste sistema.

Com efeito, se $i \neq r$, então $m_r | M_i$ e $M_i \equiv 0 (mod.m_r)$, o que implica

$$X = a_1 M_1 x_1 + a_2 M_2 x_2 + \ldots + a_k M_k x_k \equiv a_r M_r x_r (mod.m_r),$$

ísto é,

$$X \equiv a_r M_r x_r (mod.m_r)$$

e como x_r é a solução da congruência linear 2.15, temos

$$M_r x_r \equiv 1 \ (mod.m_r) \tag{2.16}$$

e multiplicando a congruência linear (2.16) por a_r, onde, $mdc(a_r, m_r) = 1$, obtemos:

$$a_r M_r x_r \equiv a_r \ (mod.m_r) \Longrightarrow X \equiv a_r (mod.m_r)$$

e isto prova que, X é uma solução do sistema 2.14 considerado.

Para demonstrar a unicidade desta solução, suponhamos que X_1 é uma outra solução qualquer do sistema de congruências considerado. Então:

$$X \equiv a_r \equiv X_1 \ (mod.m_r), \quad r = 1, 2, \ldots, k$$

de modo que $m_r | (X - X_1)$ para cada valor de r. E como o $mdc(m_i, m_j) = 1$, segue-se do corolário **??** que $m_1 m_2 \ldots m_r | (X - X_1)$, isto é:

$$m | (X - X_1) \ \ e \ X \equiv X_1 (mod.m)$$

o que termina a demonstração do "Teorema Chinês do Resto". ■

Exemplo 2.11. *Resolver o sistema de congruências lienares:*

$$\begin{cases} x & \equiv & 2 (mod\, 3) \\ x & \equiv & 3 (mod\, 5) \\ x & \equiv & 2 (mod\, 7) \end{cases}$$

Solução: Temos que $a_1 = 2$, $a_2 = 3$, $a_3 = 2$ e $m_1 = 3$, $m_2 = 5$, $m_3 = 7$. Como $mdc(m_i, m_j) = 1$ para $i \neq j$. Então, pelo Teorema Chinês do Resto 2.4, esse sistema de congruências lineares possui uma única solução módulo $m = 3 \cdot 5 \cdot 7 = 105$. E de acordo com o mesmo teorema:

$$\begin{array}{lll} M_1 = m/3 & = 5 \cdot 7 & = 35 \\ M_2 = m/5 & = 3 \cdot 7 & = 21 \\ M_3 = m/7 & = 3 \cdot 5 & = 15 \end{array}$$

e como

$$mdc(35, 3) = 1, \quad mdc(21, 5) = 1 \quad \text{e } mdc(15, 7) = 1.$$

Então pelo o corolário 2.2, os inteiros, 35, 21 e 15 possui inversos módulo 3, 5 e 7, respectivamente, de modo que temos:

$$\begin{cases} 35x \equiv 1 \ (mod\, 3) \\ 21x \equiv 1 \ (mod\, 5) \\ 15x \equiv 1 \ (mod\, 7) \end{cases} \Longrightarrow \begin{cases} 2x \equiv 1 \ (mod.3) \\ 1x \equiv 1 \ (mod.5) \\ 1x \equiv 1 \ (mod.7). \end{cases}$$

Resolvendo as congruências lineares obtemos, respectivamente,

$$x_1 = 2,\ x_2 = 1 \text{ e } x_3 = 1.$$

Portanto, pelo Teorema Chinês do Resto 2.4

$$X = a_1M_1x_1 + a_2M_2x_2 + \ldots + a_kM_kx_k$$

$$X = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233.$$

Como $233 \equiv 23\ (mod.105)$ temos que $X \equiv 23\ (mod.105)$ é a única solução incongruente módulo 105.
Portanto,

$$S = \{23 + 105k : k \in \mathbb{Z}\}$$

é o conjunto de todas as soluções deste sistema.

Teorema 2.5. *Sejam $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ e $m_1, m_2, \ldots, m_k \in \mathbb{N}$ tais que $mdc(m_i, m_j) = 1$, com $i \neq j$. Se $mdc(a_i, m_i) = 1$ para $i = 1, 2, \ldots k$. Então o sistema de congruências lineares:*

$$\begin{cases} a_1x & \equiv b_1 \quad (mod.m_1) \\ a_2x & \equiv b_2 \quad (mod.m_2) \\ a_3x & \equiv b_3 \quad (mod.m_3) \\ & \vdots \\ a_kx & \equiv b_k \quad (mod.m_k) \end{cases} \tag{2.17}$$

tem uma única solução x_0 com $1 \leq x_0 < m$, onde $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$. Além disso,

$$S = \{x_0 + km : k \in \mathbb{Z}\}$$

é o conjunto de todas as soluções deste sistema.

Prova. Como o $mdc(a_r, m_r) = 1$, então pelo teorema 2.2 a congruência linear

$$a_rx \equiv 1\ (mod\, m_r)$$

tem solução única módulo m_r que é o seu inverso, que denotaremos por $(a_r)^{-1}$, de maneira que

$$a_r(a_r)^{-1} \equiv 1(mod.m_r),\ \forall\, r = 1, 2, \ldots k.$$

Logo, a congruência linear $a_rx \equiv b_r\ (mod\, m_r)$ é equivalente à congruência

$$x \equiv b_r(a_r)^{-1}(mod.m_r)$$

e desse modo, o sistema 2.17 dado é equivalente ao sistema de congruências lineares:

$$\begin{cases} x & \equiv b_1 \cdot (a_1)^{-1} \ (mod\, m_1) \\ x & \equiv b_2) \cdot (a_2)^{-1} \ (mod\, m_2) \\ x & \equiv b_3 \cdot (a_3)^{-1} \ (mod\, m_3) \\ \vdots & \\ x & \equiv b_k \cdot (a_k)^{-1} \ (mod\, m_k). \end{cases} \tag{2.18}$$

o qual, pelo Teorema Chinês do Resto 2.4, tem uma única solução módulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$. ■

Exemplo 2.12. *Resolver o sistema de congruências lineares:*

$$\begin{cases} 2x & \equiv & 1 & (mod.5) \\ 3x & \equiv & 2 & (mod.7) \\ 4x & \equiv & 3 & (mod.11) \end{cases} \tag{2.19}$$

Solução: Os módulos $m_1 = 5$, $m_2 = 7$ e $m_3 = 11$ do sistema 2.19 dado são primos entre si dois a dois e, além disso

$$mdc(2,5) = mdc(3,7) = mdc(4,11) = 1$$

de modo que, pelo teorema 2.5, o sistema tem uma única solução módulo $m = 5 \cdot 7 \cdot 11 = 385$.

Como os inteiros, 2, 3 e 4 são inversíveis módulo 5, 7 e 11, respectivamente, temos as congruências lineares:

$$2x \equiv 1 \ (mod\, 5) \qquad 3x \equiv 1 \ (mod\, 7) \qquad \text{e} \qquad 4x \equiv 1 \ (mod\, 11)$$

tem como soluções respectivas: $x_1 = 3, x_2 = 5$ e $x_3 = 3$. De fato, pois,

$$\begin{cases} 2x & \equiv & 1 & (mod.5) \\ 3x & \equiv & 1 & (mod.7) \\ 4x & \equiv & 1 & (mod.11) \end{cases} \Longrightarrow \begin{cases} x & \equiv & 1 \cdot 2^{-1} & (mod.5) \\ x & \equiv & 1 \cdot 3^{-1} & (mod.7) \\ x & \equiv & 1 \cdot 4^{-1} & (mod.11) \end{cases} \Longrightarrow \begin{cases} x & \equiv & 1 \cdot 3 & (mod.5) \\ x & \equiv & 1 \cdot 5 & (mod.7) \\ x & \equiv & 1 \cdot 3 & (mod.11) \end{cases}$$

Portanto,

$$\begin{cases} 2x & \equiv & 1 & (mod.5) \\ 3x & \equiv & 2 & (mod.7) \\ 4x & \equiv & 3 & (mod.11) \end{cases} \Longleftrightarrow \begin{cases} x & \equiv & 3 & (mod.5) \\ x & \equiv & 10 & (mod.7) \\ x & \equiv & 9 & (mod.11) \end{cases}$$

Assim, pelo teorema 2.5 para resolver o sistema de congruências lineares 2.19 dado é suficiente resolver o sistema

$$\begin{cases} x & \equiv & 3 & (mod.5) \\ x & \equiv & 10 & (mod.7) \\ x & \equiv & 9 & (mod.11) \end{cases}$$

e pelo teorema 2.5, com $M_1 = 77, M_2 = 55$ e $M_3 = 35$; e $x_1 = 3$, $x_2 = 6$ e $x_3 = 6$, onde

$$X = 3 \cdot 77 \cdot 3 + 10 \cdot 55 \cdot 6 + 9 \cdot 35 \cdot 6 = 5883.$$

Portanto, $X \equiv 108\ (mod.385)$ é a única solução do sistema de congruências lineares 2.19.

O próximo resultado resolve de maneira mais geral o nosso problema.

Teorema 2.6. *Seja $n \in \mathbb{N}$. Sejam $c_1, \ldots, c_n \in \mathbb{Z}$ e $m_1, \ldots, m_n \in \mathbb{Z}_+^*$ e considere o sistema de equações:*

$$\begin{cases} x \equiv c_1 \quad (mod\, m_1) \\ \vdots \\ x \equiv c_n \quad (mod\, m_{n)}. \end{cases} \tag{2.20}$$

A condição necessária e suficiente para que (2.20) admita solução é que, para quaisquer $i, j \in \{1, 2, \ldots, n\}$ tenhamos $d|(c_i - c_j)$ sendo $d = mdc\,(m_i, m_j)$.

Quando (2.20) admite solução, ela é única módulo $mmc\,(m_1, \ldots, m_n)$.

Prova. Primeiramente, suponha que x_0 e y_0 são soluções de (2.20). Vamos mostrar que

$$y_0 \equiv x_0\ (mod\, mmc\,(m_1, \ldots, m_n)).$$

Consequentemente, x_0 e y_0 sendo soluções de (2.20) nos diz que $x_0 \equiv c_j\ (mod\, m_j)$ e $y_0 \equiv c_j\ (mod\, m_j)$ para todo $j \in \{1, \ldots, n\}$.

Logo,

$$y_0 - x_0 \equiv 0\ (mod\, m_j) \quad (\text{para todo } j \in \{1, \ldots, n\})$$

de onde concluímos que $y_0 - x_0$ é múltiplo de todos os $m_j\ (j \in \{1, \ldots, n\})$, logo, $(y_0 - x_0)$ é um múltiplo do $mmc\,(m_1, \ldots, m_n)$, ou seja,

$$y_0 \equiv x_0\ (mod\, mmc\,(m_1, \ldots, m_n)).$$

Concluímos então que se (2.20) admite solução ela é única módulo $mmc\,(m_1, \ldots, m_n)$.

Em seguida, mostraremos que a condição enunciada é necessária. Com efeito, se x_0 é solução de (2.20), para quaisquer $i, j \in \{1, \ldots, n\}$ temos

$$\begin{aligned} &(1)\ x_0 \equiv c_i \quad (mod\, m_i) \\ &(2)\ x_0 \equiv c_j \quad (mod\, m_j). \end{aligned}$$

De acordo com a definição 1.7 existe $t \in \mathbb{Z}$ tal que (1) pode ser escrita como $x_0 - c_i = m_i t$ o que implica $x_0 = c_i + m_i t$. Substituindo essa informação em (2), obtemos $c_i + m_i t \equiv c_j \ (mod\, m_j)$, como $-c_i \equiv -c_i \ (mod\, m_j)$ consequentemente escrevemos

$$m_i t \equiv (c_j - c_i) \ (mod\, m_j).$$

Então a equação de congruência

$$m_i y \equiv (c_j - c_i) \ (mod\, m_j)$$

admite solução $y = t$. Logo, pelo teorema 2.1, temos que $d|(c_j - c_i)$ sendo $d = mdc\,(m_j, m_i)$.

Finalizaremos agora com a última parte da demonstração, que essencialmente, será feita por indução sobre o número n de equações de (2.20). O procedimento é o seguinte: em primeiro lugar provamos que a condição enunciada no teorema é suficiente se $n = 2$. Depois, aplicamos este resultado nas duas primeiras equações do sistema (admitindo $n > 2$) e mostramos que as duas equações podem ser transformadas (preservando as soluções) em apenas uma nova equação. Por fim, verificamos que o novo sistema de $n-1$ equações de congruência assim obtido satisfaz as mesmas condições do sistema original e o resultado segue por indução. ■

Afirmação 2.1. *Suponha que $n = 2$ em (2.20), ou seja, o sistema (2.20) tem a forma*

$$\begin{cases} x \equiv c_1 \quad (mod\, m_1) \\ x \equiv c_2 \quad (mod\, m_2), \end{cases} \tag{2.21}$$

e a condição $d|(c_1 - c_2)$ sendo $d = mdc\,(m_1, m_2)$ garante existência de solução para este sistema.

Prova. Considere a uma solução da congruência $x \equiv c_1 \ (mod\, m_1)$. Então pela definição 1.7 existe $b \in \mathbb{Z}$ tal que

$$a - c_1 = bm_1,$$

ou,

$$a = c_1 + bm_1.$$

Substituindo essa informação na segunda equação do sistema obtemos a equação

$$c_1 + bm_1 \equiv c_2 \ (mod\, m_2)$$

por ser $-c_1 \equiv -c_1 \ (mod\, m_2)$ somamos ordenadamente as congruências e obtemos

$$bm_1 \equiv c_2 - c_1 \ (mod\, m_2)$$

que é equivalente a equação

$$m_1 b \equiv (c_2 - c_1) \ (mod\, m_2)$$

e por hipótese temos que $d = mdc\,(m_2, m_1)$ e $d|(c_2 - c_1)$, logo a equação acima admite solução b_0 e observe que $f = c_1 + b_0 m_1$, é solução do sistema (2.21), como é possível verificar. ■

Afirmação 2.2. *Considere o sistema (2.21). Seja f uma solução deste sistema. Então $g \in \mathbb{Z}$ é solução do sistema se, e somente se, é solução da equação*

$$g \equiv f \ (mod\, mmc\,(m_1, m_2)).$$

Prova. Seja $g \in \mathbb{Z}$ uma outra solução do sistema (2.21). Já vimos que a solução é única módulo o MMC. Consequentemente, com $n = 2$ temos

$$g \equiv f \ (mod\, mmc\,(m_1, m_2)).$$

Reciprocamente, temos que a congruência acima implica que

$$g \equiv f \ (mod\, m_1) \Longrightarrow g \equiv c_1 \ (mod\, m_1).$$

Analogamente, $g \equiv c_2 \ (mod\, m_2)$, logo g é solução do sistema. ■

Afirmação 2.3. *Considere o sistema*

$$\begin{cases} x \equiv c_1 & (mod\, m_1) \\ x \equiv c_2 & (mod\, m_2) \\ \vdots & \\ x \equiv c_n & (mod\, m_n), \end{cases}$$

com $n \geq 3$. Onde de acordo com o teorema, supomos que o $mdc\,(m_i, m_j)|(c_i - c_j)$ para todos $i, j \in \{1, \ldots, n\}$. E como já vimos, baseados nas afirmações (2.1) e (2.2) podemos transformar as duas primeiras equações do sistema acima em apenas uma, obtendo consequentemente o sistema

$$\begin{cases} x \equiv f & (mod\, mmc\,(m_1, m_2)) \\ x \equiv c_3 & (mod\, m_3) \\ \vdots & \\ x \equiv c_n & (mod\, m_n). \end{cases} \tag{2.22}$$

Então para todo $i \in \{3, \ldots, n\}$, temos que o $mdc\,(m_i, mmc\,(m_1, m_2))$ divide $(c_i - f)$.

Prova. Inicialmente precisamos fixar $i \in \{1, \ldots, n\}$. Em seguida, consideramos p um primo qualquer que divide o módulo m_i, por outro lado, tome β_j a potência máxima de p que

divide m_j, com $j \in \{1, \ldots, n\}$. Como queremos saber qual a potência máxima de p que divide o $mdc\,(m_i, mmc\,(m_1, m_2))$, podemos afirmar, que a potência máxima de p que divide o $mmc\,(m_i, m_j)$ é $max\{\beta_i, \beta_j\}$ enquanto que a potência máxima de p que divide o $mdc\,(m_i, m_j)$ é o $min\{\beta_i, \beta_j\}$. Assim, concluímos que a potência máxima de p que divide o máximo divisor comum entre m_i e o $mmc\,(m_1, m_2)$ é

$$\alpha = min\{\beta_i, max\{\beta_1, \beta_2\}\}.$$

Supondo que β_1 seja a potência máxima de p que divide o $mmc\,(m_1, m_2)$ teríamos então que encontrar $\alpha = min\{\beta_i, \beta_1\}$, contudo, se tomarmos β_2 a potência máxima de p que divide o $mmc\,(m_1, m_2)$ teríamos que encontrar $\alpha = min\{\beta_i, \beta_2\}$. Mas, como queremos encontrar a potência máxima de p entre as duas potências mínimas, escrevemos a seguinte igualdade

$$\begin{aligned} \alpha &= min\{\beta_i, max\{\beta_1, \beta_2\}\} = \\ &= max\{min\{\beta_i, \beta_1\}, min\{\beta_i, \beta_2\}\}, \end{aligned}$$

ou seja p^α é a potência máxima de p que divide o $mdc\,(m_i, mmc\,(m_1, m_2))$.

Portanto, para concluirmos que o $mdc(m_i, mmc\,(m_1, m_2))$ divide $(c_i - f)$, é suficiente provar que cada potência máxima de primo p^α, que divide $mdc\,(m_i, mmc\,(m_1, m_2))$, também divide $(c_i - f)$.

Por hipótese, temos que $p^{min\{\beta_1, \beta_i\}}$ divide $(c_1 - c_i)$, já que $p^{min\{\beta_1, \beta_i\}}$ divide $mdc\,(m_1, m_i)$ e o $mdc\,(m_1, m_i)$ divide $(c_1 - c_i)$. De forma análoga, a potência $p^{min\{\beta_2, \beta_i\}}$ divide $(c_2 - c_i)$, pois, $p^{min\{\beta_2, \beta_i\}}$ divide o $mdc\,(m_2, m_i)$ que divide $(c_2 - c_i)$.

$$p^{\beta_1} | (c_1 - f) \text{ pois } f \equiv c_1 \ (mod\, m_1)$$

e

$$p^{\beta_2} | (c_2 - f) \text{ pois } f \equiv c_2 \ (mod\, m_2).$$

Escrevendo

(1) $c_i - f = (c_i - c_1) + (c_1 - f)$
(2) $c_i - f = (c_i - c_2) + (c_2 - f)$,

observamos que a potência $p^{min\{\beta_1, \beta_i\}}$ divide $c_i - f$ e a potência $p^{min\{\beta_2, \beta_i\}}$ também divide $c_i - f$. Logo p^α divide $(c_i - f)$.

Agora, a conclusão da demonstração do teorema 2.6 segue por indução. O caso $n = 2$ foi demonstrado na afirmação 2.1 e para o caso geral $n > 2$ tomamos o sistema inicial 2.20 e passamos através das afirmações (2.2) e (2.3) para o sistema (2.22) que satisfaz as mesmas

condições do sistema 2.20 mas, tem apenas $(n-1)$ equações. Por hipótese de indução o sistema 2.22 tem solução e esta solução é a mesma do sistema 2.20. Isso acaba a demonstração do teorema 2.6. ■

A seguir ilustraremos as descrições feitas no teorema através de exemplos.

Exemplo 2.13. *Verifique se o sistema seguinte tem solução e, caso tenha, obtenha estas soluções:*

$$\begin{cases} x \equiv 3 \quad (mod\, 4) \\ x \equiv 5 \quad (mod\, 2). \end{cases} \tag{2.23}$$

Solução: Temos que o $mdc\,(2,4) = 2$ e $2|(5-3)$ logo, este sistema admite solução única módulo $mmc\,(2,4) = 4$. Com efeito, encontraremos esta solução seguindo os passos da demonstração do teorema 2.6. Inicialmente, tomamos a primeira equação deste sistema

$$x \equiv 3 \quad (mod\, 4)$$

e utilizando a definição 1.7 temos $4|(x-3) \Rightarrow \exists\, t \in \mathbb{Z}$ tal que $x-3 = 4t \Longrightarrow x = 3+4t$, e uma solução para a primeira equação é do tipo $f = 3+4t$, assim precisamos encontrar t tal que f seja também solução da segunda equação, ou seja, substitua o valor de x na equação

$$x \equiv 5\ (mod\, 2)$$

obtendo

$$3+4t \equiv 5 \quad (mod\, 2)$$

como $-3 \equiv -3\ (mod\, 2)$, pela propriedade (2) do teorema 1.9, somamos ordenadamente com a congruência acima

$$3+4t-3 \equiv 5-3 \quad (mod\, 2)$$

e obtemos

$$4t \equiv 2\ (mod\, 2),$$

como o $mdc\,(4,2) = 2$ podemos reescrever 2 como combinação linear de 4 e 2, logo

$$2 = 1.4 - 1.2$$

ou seja, $4.1 \equiv 2\ (mod\, 2)$.

Portanto $t \equiv 1\ (mod\, 2)$ é uma solução, e $f = 3+4.1 = 7$ é uma solução para o sistema 2.23 original.

Exemplo 2.14. *Verifique se os sistemas seguintes têm solução e, caso tenham, obtenha estas soluções:*

$$\begin{cases} x \equiv 3 & (mod\, 4) \\ x \equiv 7 & (mod\, 6) \\ x \equiv 10 & (mod\, 5) \end{cases} \tag{2.24}$$

e

$$(II) \quad \begin{cases} x \equiv 2 & (mod\, 3) \\ x \equiv 3 & (mod\, 5) \\ x \equiv 2 & (mod\, 7) \end{cases}$$

Solução: Aqui iremos usar o passos descritos no teorema 2.6, tendo em vista, que o sistema (II) tem uma particularidade: os módulos 3, 5, e 7 são co-primos, ou seja, o maior divisor comum entre eles é um.

Passemos então a resolução do sistema (I).

Temos que o $mdc\,(4,6) = 2$ e $2|(7-3)$; o $mdc\,(6,5) = 1$ e $1|(10-7)$; o $mdc\,(4,5) = 1$ e $1|(10-3)$. Logo, este sistema admite solução única módulo $mmc\,(4,5,6) = 60$.

Considere primeiramente o sistema:

$$\begin{cases} x \equiv 3 & (mod\, 4) \\ x \equiv 7 & (mod\, 6), \end{cases} \tag{2.25}$$

da primeira equação, existe $t \in \mathbb{Z}$ tal que $x - 3 = 4t \Longrightarrow x = 3 + 4t$ e podemos afirmar, que uma solução para tal equação é do tipo $f = 3 + 4t$, $\forall t \in \mathbb{Z}$. Agora precisamos determinar t para que f seja solução da segunda equação, ou seja,

$$3 + 4t \equiv 7 \quad (mod\, 6),$$

como $-3 \equiv -3\ (mod\, 6)$, pelo teorema 1.9, podemos somar ordenadamente com a equação acima

$$3 + 4t - 3 \equiv 7 - 3\ (mod\, 6)$$

obtendo,

$$4t \equiv 4\ (mod\, 6),$$

logo $t = 1$ é solução e, $f = 3 + 4.1 = 7$ é uma solução deste sistema parcial (2.25).

Como o $mmc\,(4,6) = 12$, podemos substituir estas duas equações por $x \equiv 7\ (mod\, 12)$, e então resolver o sistema

$$\begin{cases} x \equiv 7 & (mod\, 12) \\ x \equiv 10 & (mod\, 5). \end{cases} \tag{2.26}$$

Fazendo o mesmo procedimento para o sistema acima, obtemos da primeira equação $x = 7 + 12t$, donde podemos escrever $g = 7 + 12t$ uma solução para $x \equiv 7 \ (mod\, 12)$, que substituida na segunda, nos dá

$$7 + 12t \equiv 10 \ (mod\, 5) \tag{2.27}$$

e como $-7 \equiv -7 \ (mod\, 5)$, pela a propriedade (2) do teorema 1.9, a equação 2.27 acima, é equivalente a

$$12t \equiv 3 \ (mod\, 5).$$

Como o $mdc\,(12, 5) = 1$, reescrevemos 1 como uma combinação linear de 12 e 5

$$1 = 3.12 - 7.5,$$

multiplicando ambos os membros da igualdade por 3, temos:

$$3 = 9.12 - 21.5,$$

ou seja,

$$12.9 \equiv 3 \ (mod\, 5).$$

Portanto $t \equiv 9 \ (mod\, 5)$ é uma solução, e $g = 7 + 12.9 = 115$ é uma solução para o sistema 2.24 original.

A seguir resolveremos o sistema (II).

Tome o sistema

$$\begin{cases} x \equiv 2 \quad (mod\, 3) \\ x \equiv 3 \quad (mod\, 5) \\ x \equiv 2 \quad (mod\, 7) \end{cases} \tag{2.28}$$

e observe que neste, existe entre os módulos uma particularidade: são primos entre si. Logo, iremos verificar se para este caso o teorema 2.6 também é válido.

Solução: O $mdc\,(3, 5) = 1$ e divide $(3 - 2)$, o $mdc\,(3, 7) = 1$ e divide $(2 - 2)$ e por fim, o $mdc\,(5, 7) = 1$ e divide $(3 - 2)$ então o sistema dado admite solução única módulo $mmc\,(3, 5, 7) = 105$.

Como já vimos, vamos considerar inicialmente o sistema com as duas primeiras equações

$$\begin{cases} x \equiv 2 \quad (mod\, 3) \\ x \equiv 3 \quad (mod\, 5) \end{cases}$$

Com efeito, da equação $x \equiv 2 \pmod 3$ obtemos $x = 2+3t$, e com isso, uma solução do tipo $f = 2+3t$ que satisfaz a primeira equação deste sistema, quaisquer que seja $t \in \mathbb{Z}$. Agora precisamos determinar $t \in \mathbb{Z}$ tal que f seja solução da segunda equação, isto é,

$$2+3t \equiv 3 \pmod 5$$

e pelo o teorema 1.9 esta equação é equivalente a

$$\begin{array}{lll} 3t \equiv 1 & (mod\,5), & \text{como } 1 \equiv 6\ (mod\,5) \\ 3t \equiv 6 & (mod\,5) & \text{e} \\ 3.t \equiv 3.2 & (mod\,5) & \text{e por ser o mdc}\,(3,5)\text{=1} \\ t \equiv 2 & (mod\,5) & \end{array}$$

logo $t = 2$ é solução, e assim $f = 2+3.2 = 8$ é uma solução deste sistema parcial.

Como o $mmc\,(3,5) = 15$, podemos substituir estas duas equações por $x \equiv 8\ (mod\,15)$, e então resolver o sistema

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod 7, \end{cases}$$

e daqui iniciar o procedimento já realizado para os sistemas anteriores.

Todavia, encontramos uma solução do tipo $g = 8+15t$ que satisfaz a primeira equação do sistema acima. Em seguida, substituimos na segunda equação obtendo

$$8+15t \equiv 2 \pmod 7$$

e esta equação é equivalente a

$$15t \equiv -6\ (mod\,7)$$

como $-6 \equiv 15\ (mod\,7)$

$$15t \equiv 15\ (mod\,7).$$

Como o $mdc\,(15,7) = 1$, e podemos reescrever 1 como uma combinação linear de 15 e de 7, temos

$$1 = 1.15 - 2.7$$

então, multiplicando ambos os membros da igualdade por 15

$$15 = 15.15 - 30.7,$$

ou seja,

$$15.15 \equiv 15\ (mod\,7).$$

Portanto $t \equiv 15 \ (mod\, 7)$ é uma solução, e $g = 8 + 15.15 = 233$ é uma solução do sistema 2.28 original.

2.3 Teorema de Lagrange

A seguir veremos um resultado que relaciona o número de soluções módulo m de um polinômio $f(x) \in \mathbb{Z}[x]$ com o grau deste polinômio.

Teorema 2.7. *[Teorema de Lagrange]Sejam*

$$f(x) = a_k x^k + \ldots + a_1 x + a_0$$

um polinômio inteiro de grau k e $p \in \mathbb{N}$ *um primo tal que* $a_k \not\equiv 0 \ (mod\, p)$. *Então a equação* $f(x) \equiv 0 \ (mod\, p)$ *tem no máximo k soluções incongruentes módulo p (isto é, existem* $m \leq k$ *inteiros* $t_1, \ldots, t_m$ *tais que* $f(t_i) \equiv 0 \ (mod\, p)$ *para* $i \in \{1, \ldots, m\}$, *e* $t_i \not\equiv t_j \ (mod\, p)$ *para* $i, j \in \{1, \ldots, k\}$, $i \neq j$).

Prova. Para a demonstração deste teorema, iremos utilizar o Princípio de indução matemática sobre o grau k do polinômio $f(x)$.

Se temos $k = 0$ então $f(x) = a_0$ é um polinômio constante e $a_0 \not\equiv 0 \ (mod.p)$, por hipótese. Logo, concluímos que $f(x) \equiv 0 \ (mod.p)$ não admite solução, o que neste caso, o teorema fica provado.

Suponhamos agora, por hipótese de indução, que o teorema é verdadeiro para qualquer polinômio de grau menor ou igual a $k-1$ e mostraremos que o teorema é válido para grau k.

Obviamente, se $f(x)$ não tem raiz módulo p, o teorema é válido.

Suponha então que existe $a \in \mathbb{Z}$ uma raiz de $f(x)$ módulo p. Pelo teorema 1.11 da fatoração, podemos escrever $f(x) \equiv (x-a).g(x) \ (mod\, p)$, onde $g(x)$ tem grau $k-1$. Logo, podemos afirmar que, qualquer raiz de $f(x)$ ou é raiz de $(x-a)$ ou é raiz de $g(x)$ (pois, para quaisquer polinômio $f(x), g(x), g_1(x) \in \mathbb{Z}[x]$, se $f(x) \equiv g(x).g_1(x) \ (mod\, p)$ então qualquer raiz de $f(x)$ módulo p é raiz de $g(x)$ ou $g_1(x)$ módulo p). Agora, $(x-a)$ tem uma única raiz módulo p, enquanto que $g(x)$, pela a hipótese de indução, tem no máximo $k-1$ raízes incongruentes módulo p, logo, $f(x)$ tem no máximo k raízes incongruentes módulo p. ■

Exemplo 2.15. *Verifique, a partir do teorema de Lagrange, a quantidade de soluções da equação*

$$f(x) = 5x^2 - 3x + 16 \equiv 0 \ (mod\, 2)$$

Solução: De acordo com o teorema 2.7, a equação acima admite 2 soluções incongruentes módulo 2, pois, o $5 \not\equiv 0 \ (mod\, 2)$. Assim:
para $x = 0$, temos $f(0) = 5 \cdot 0^2 - 3 \cdot 0 + 16 = 16 \equiv 0 \ (mod\, 2)$
para $x = 1$, temos $f(1) = 5 \cdot 1^2 - 3 \cdot 1 + 16 = 18 \equiv 0 \ (mod\, 2)$

para $x = 2$, temos $f(2) = 5 \cdot 2^2 - 3 \cdot 2 + 16 = 30 \equiv 0 \ (mod\, 2)$
para $x = 3$, temos $f(3) = 5 \cdot 3^2 - 3 \cdot 3 + 16 = 52 \equiv 0 \ (mod\, 2)$.

Observe que $0 \not\equiv 1 \ (mod\, 2)$ e $2 \not\equiv 3 \ (mod\, 2)$, como $0 \equiv 2 \ (mod\, 2)$ e $1 \equiv 3 \ (mod\, 2)$, podemos concluir que, todo $x \in \mathbb{Z}$ solução de $f(x)$ será congruente a 0 ou a 1 módulo 2.

3 Equações de Congruência de Grau Maior que Um

Neste capítulo continuaremos estudando as equações de congruência. Essencialmente, para algum $m \in \mathbb{Z}_+^*$, estaremos preocupados em investigar a solubilidade (em $\mathbb{Z}$) de equações do tipo $a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (mod\, m)$, bem como, os sistemas de tais equações.

3.1 Equações de Grau Maior que Um

Consideramos a equação de congruência do tipo

$$f(x) \equiv 0 \ (mod\, m) \tag{3.1}$$

onde o polinômio $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ é um polinômio primitivo de grau $n \in \mathbb{N}$ e m é um inteiro positivo.

Estaremos interessados principalmente em determinar se uma equação deste tipo admite ou não solução (de fato, construíremos um processo algorítmico para obter soluções da equação 3.1) sem nos preocuparmos muito com a quantidade destas soluções.

A seguir, faremos um passo a passo de como resolver a equação 3.1.

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (mod\, m)$$

3.2 Algoritmo

Algoritmo

1. Decomponha o módulo m em fatores primos. Considere m da forma, $m = p^{\alpha}$.
2. Encontre a solução para $\alpha = 1$, isto é, $f(x_0) \equiv 0 \ (mod\, p)$.

3. Substitua a solução encontrada na equação $f(x_0+pt)\equiv 0\ (mod\, p^2)$, com $\alpha=2$.
4. Encontrar o valor de t, para que seja solução de $f(x_0+pt)\equiv 0\ (mod\, p^2)$.

   i) Para isso utilize o desenvolvimento de Taylor[1] de $f(x)$ de ordem n numa vizinhança de um ponto $x=x_0$, que é dado por $f(x)=P_n(x)+R_n(x)$;[2] O que implica que,

$$f(x)=f(x_0)+\frac{f^{'}(x_0)}{1!}(x-x_0)+...+\frac{f^{(n)}(x_0)}{n!}(x-x_0)^n. \tag{3.2}$$

   ii) Substituindo $x=x_0+pt$ no desenvolvimento de Taylor acima e aplicando o módulo p^2 obtemos a congruência

$$f(x_0+pt)\equiv f(x_0)+f^{'}(x_0)pt\equiv 0\ (mod\, p^2),\quad com\ \alpha\in\mathbb{N}. \tag{3.3}$$

   iii) Encontre e resolva a congruência linear;

$$f^{'}(x_0)t\equiv -\frac{f(x_0)}{p^2}\ (mod\, p). \tag{3.4}$$

   Determinando portanto, o valor de t.
5. Indutivamente, considere $\beta\in\mathbb{N}$, $\beta<\alpha$ e $c\in\mathbb{Z}$ uma solução da equação

$$f(x)\equiv 0\ (mod\, p^{\beta}). \tag{3.5}$$

   Para qualquer $t\in\mathbb{Z}$ temos que $(c+tp^{\beta})^k$ é igual a

$$c^k+\binom{k}{1}c^{k-1}(tp^{\beta})+\ldots+\binom{k}{j}c^{k-j}(tp^{\beta})^j+\ldots+(tp^{\beta})^k\equiv c^k\ (mod\, p^{\beta}),$$

   logo,

$$0\equiv f(c)\equiv f(c+tp^{\beta})\ (mod\, p^{\beta})$$

   ou seja, $c+tp^{\beta}$ também é solução de (3.5). Queremos agora determinar $t\in\mathbb{Z}$ tal que $c+tp^{\beta}$ seja uma solução da equação

$$f(c+tp^{\beta})\equiv 0\ (mod\, p^{\beta+1}). \tag{3.6}$$

---

[1] ver o livro: Introdução à Análise Real/Aldo Bezerra Maciel; Osmundo Alves Lima. - Campina Grande: EDUEP, 2005, p.173

[2] onde, $R_n(x)=\dfrac{f^{n+1}(a)}{(n+1)!}=0$, pois, $f^{n+1}(x)$ é identicamente zero, posto que, $f(x)$ é um polinômio em $\mathbb{Z}[x]$ de grau n.

Podemos então reescrever a equação (3.6) utilizando o desenvolvimento de Taylor de $f(x)$, tomando $x = c + tp^{\beta}$ e assim teremos,

$$f(c+tp^{\beta}) \equiv f(c) + f^{'}(c)tp^{\beta} \equiv 0 \ (mod\, p^{\beta+1}) \tag{3.7}$$

já que, no desenvolvimento de $f(c+tp^{\beta})$ acima, todas as potências de p a partir do terceiro termo são maiores que $\beta+1$.

Como $f(c) \equiv 0 \ (mod\, p^{\beta})$, concluímos que $\dfrac{f(c)}{p^{\beta}} \in \mathbb{Z}$, e usando esta informação na equação acima obtemos a equação linear

$$f^{'}(c)t \equiv -\frac{f(c)}{p^{\beta}} \ (mod\, p) \tag{3.8}$$

cujo número de soluções já conhecemos (teorema 2.1), qual seja (veja que o $mdc\,(f^{'}(c), p) = 1$ ou p) :

$$\begin{cases} 0 & \text{se } p|f^{'}(c) \text{ e } p \nmid (f(c)/p^{\beta}) \\ 1 & \text{se } p \nmid f^{'}(c) \\ p & \text{se } p|f^{'}(c) \text{ e } p|(f(c)/p^{\beta}). \end{cases}$$

O procedimento geral deve ser agora claro. Se todas as soluções de (3.8) são conhecidas para o caso $\beta = 1$, escolhemos uma delas, que denotaremos por c_1. Substituindo c por c_1 em (3.7), e repetindo o processo para o caso $\beta = 2$, buscaremos uma solução para (3.8), agora com c_1 no lugar de c, e assim por diante até encontrarmos a solução de (3.5), com o β desejado, ou seja, $\beta + 1 = \alpha$.

Caso o número de soluções da congruência linear (3.8) obtido seja zero, escolhe-se outro c_1. Se nenhuma das soluções de (3.8) para o caso $\beta = 1$ induz (através deste processo) uma solução de (3.7) para o caso $\beta = 2$, é porque não existe tal solução (uma solução para o caso $\beta = 2$ é também solução para o caso $\beta = 1$).

Vamos ilustrar este processo, num caso particular para $\alpha = 3$.

Seja p um primo, $\alpha \in \mathbb{N}$ e $f(x) \in \mathbb{Z}[x]$ um polinômio primitivo de grau n.

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (mod\, p^{\alpha}),$$

a partir das soluções da equação

$$f(x) \equiv 0 \ (mod\, p).$$

Vamos supor que seja possível encontrar soluções para a equação 3.1 no caso particular onde m é da forma p^{α}, com $\alpha = 3$, ou seja, vamos resolver a equação

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (mod\, p^3). \tag{3.9}$$

O que faremos a seguir é aplicar os procedimentos do algoritmo para construirmos uma solução para $f(x) \equiv 0 \ (mod\, p^\alpha)$.

Seguindo os passos descritos no procedimento acima, temos que:

1° Passo - o módulo da equação 3.9 é da forma $m = p^3$

2° Passo - vamos encontrar a solução para $\alpha = 1$, sendo assim, precisamos encontrar, primeiramente, uma solução para a equação

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (mod\, p). \tag{3.10}$$

Considere $x = x_0$ uma solução para esta equação, logo podemos dizer que $x \equiv x_0 \ (mod\, p)$ mas, de acordo com o teorema 2.1 $x = x_0 + pt$ também é solução para todo $t \in \mathbb{Z}$, ou seja,

$$f(x_0 + pt) \equiv 0 \ (mod\, p).$$

De fato, pelo binômio de Newton constatamos que, para $k = 1, \ldots n$, temos que

$$(x_0 + pt)^k = x_0^k + \binom{k}{1} x_0^{k-1}(pt) + \ldots + \binom{k}{j} x_0^{k-j}(pt)^j + \ldots + (pt)^k.$$

Como $pt \equiv 0 \ (mod\, p)$ e aplicando os conceitos de congruência no segundo membro da equação acima, obtemos que

$$x_0^k + 0 + \ldots + 0 + \ldots + 0 \equiv x_0^k \ (mod\, p),$$

logo, por transitividade,

$$(x_0 + pt)^k \equiv x_0^k \ (mod\, p).$$

Portanto,

$$f(x_0 + pt) \equiv f(x_0) \equiv 0 \ (mod\, p),$$

ou seja, $x_0 + pt$ também é solução de 3.10.

3º Passo - Queremos agora determinar $t \in \mathbb{Z}$ tal que $x_0 + pt$ seja uma solução da equação

$$f(x_0 + pt) \equiv 0 \ (mod\, p^2). \tag{3.11}$$

4º Passo/item i **-** Vamos utilizar o desenvolvimento de Taylor de $f(x)$ no ponto $x = x_0$, para encontrar o valor de t. Assim,

$$f(x) = f(x_0) + f^{'}(x_0)(x-x_0) + \frac{f^{''}(x_0)}{2!}(x-x_0)^2 + \ldots + \frac{f^{(k)}(x_0)}{k!}(x-x_0)^n.$$

Substituindo $x = x_0 + pt$ obtemos,

$$f(x_0+pt) = f(x_0) + f^{'}(x_0)(x_0+pt-x_0) + f^{''}(x_0)(x_0+pt-x_0)^2 + \ldots + f^{(k)}(x_0)(x_0+pt-x_0)^k.$$

ou ainda,

$$f(x_0+pt) = f(x_0) + f^{'}(x_0)(pt) + f^{''}(x_0)(pt)^2 + \ldots + f^{(k)}(x_0)(pt)^k,$$

distribuindo a potência, temos

$$f(x_0+pt) = f(x_0) + f^{'}(x_0)(pt) + f^{''}(x_0)(p^2t^2) + \ldots + f^{(k)}(x_0)(p^kt^k),$$

utilizando o conceito de congruências, obtemos

$$f(x_0+pt) \equiv f(x_0) + f^{'}(x_0)(pt) + f^{''}(x_0).0.t^2 + \ldots + f^{(k)}(x_0).0.t^k \equiv 0 \ (mod\, p^2).$$

4° Passo/item *ii* - Encontramos então, a seguinte congruência,

$$f(x_0+pt) \equiv f(x_0) + f^{'}(x_0)pt \equiv 0 \ (mod\, p^2), \tag{3.12}$$

já que no desenvolvimento de $f(x_0+pt)$ acima, todas as potências de p, a partir da terceira parcela desta soma, são maiores ou iguais que a potência do módulo p^2.

Tome,

$$f(x_0) + f^{'}(x_0)pt \equiv 0 \ (mod\, p^2),$$

como $f(x_0) \equiv 0 \ (mod\, p)$, ou seja, $p|f(x_0)$, concluímos que $\frac{f(x_0)}{p} \in \mathbb{Z}$, e pelo o teorema 1.9 item (2), obtemos,

$$f^{'}(x_0)pt \equiv -\frac{f(x_0)}{p} \ (mod\, p^2).$$

Logo, observe que, além de $f(x_0)$ ser divisível por p, os inteiros $f^{'}(x_0)pt$ e p^2 também são. Assim, utilizando o teorema 1.8 item (3) (passamos para o proxímo passo.)

4° Passo/item *iii* - Encontramos a equação de congruência linear

$$f^{'}(x_0)t \equiv -\frac{f(x_0)}{p} \ (mod\, p) \tag{3.13}$$

e devemos verificar se esta equação admite ou não soluções. Sendo assim, observamos que o $mdc(f'(x_0), p) = 1$ ou p.
Usando o teorema 2.1 detectamos que:

- se o $mdc(f'(x_0), p) = p$ e p não divide $\frac{f(x_0)}{p}$ a equação não admite solução;
- se $f'(x_0)$ e p forem primos entre si, p não divide $f'(x_0)$ e a equação admite uma única solução incongruente módulo p;
- se o $mdc(f'(x_0), p) = p$ e p divide $\frac{f(x_0)}{p}$ então a equação admite exatamente p soluções incongruentes módulo p.

Todavia, considere que a equação 3.13 admite pelo menos uma solução $y \in \mathbb{Z}$. Logo,

$$t \equiv y \ (mod\, p)$$

e pela definição 1.7 existe $t_1 \in \mathbb{Z}$ tal que, $t = y + pt_1$ que substituido em $x = x_0 + pt$ obtemos,

$$x = x_0 + p(y + pt_1) = (x_0 + py) + p^2 t_1 = q + p^2 t_1,$$

onde, $q = (x_0 + py) \in \mathbb{Z}$ então $x = q + p^2 t_1$ é uma solução para

$$f(q + p^2 t_1) \equiv 0 \ (mod\, p^2).$$

Observação: - Fizemos, até aqui, todos os passos do Algoritmo para encontrarmos uma solução para $f(x) \equiv 0 \ (mod\, p^2)$.

Mas, como o nosso objetivo é encontrarmos uma solução para

$$f(x) \equiv 0 \ (mod\, p^3).$$

(pois, queremos obter uma solução para o caso em que $\alpha = 3$) iremos realizar o mesmo procedimento a partir do **3º Passo**.

3º Passo - Agora tentaremos obter $t_1 \in \mathbb{Z}$ para que

$$f(q + p^2 t_1) \equiv 0 \ (mod\, p^3).$$

4º Passo/item *ii* **-** Utilizando novamente Taylor, obtemos

$$f(q) + f'(q) p^2 t_1 \equiv 0 \ (mod\, p^3)$$

Como $f(q) \equiv 0 \ (mod\, p^2)$, pela definição 1.7, $\frac{f(q)}{p^2} \in \mathbb{Z}$, e pelos respectivos teoremas 1.9 item 2 e 1.8 item 3, obtemos a congruência linear

$$f'(q) t_1 \equiv -\frac{f(q)}{p^2} \ (mod\, p)$$

como o $mdc(f'(q), p) = 1$ ou p, precisamos verificar se a equação acima admite ou não soluções:

- se o $mdc(f'(q), p) = p$ e p não divide $\frac{f(q)}{p^2}$ a equação não admite solução;
- se $f'(q)$ e p forem primos entre si, p não divide $f'(q)$ e a equação admite uma única solução;
- se o $mdc(f'(q), p) = p$ e p divide $\frac{f(q)}{p^2}$ então a equação admite exatamente p soluções.

Considere que a equação acima admite ao menos uma solução z. Então,

$$t_1 \equiv z \ (mod\, p).$$

Tomando $t_1 = z$ encontramos $x = q + p^2 t_1 = q + p^2 z$, e escrevendo $k = q + p^2 z \in \mathbb{Z}$ temos $x = k$, ou seja, $x \equiv k \ (mod\, p^3)$ é raiz de

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (mod\, p^3).$$

A seguir ilustraremos o que foi apresentado com um exemplo.

Exemplo 3.1. *Usando todos os passos descritos no Algoritmo obtenha uma solução para*

$$f(x) = 5x^2 - 3x + 16 \equiv 0 \ (mod\, 8). \tag{3.14}$$

Solução: Como já vimos anteriormente, precisamos determinar uma solução para

$$f(x) \equiv 0 \ (mod\, 8)$$

e para isto, seguiremos o caminho descrito no algoritmo determinando primeiramente uma solução módulo 2.

1º Passo - o módulo da equação 3.14 é da forma $m = 2^3$

2° Passo - vamos encontrar a solução para $\alpha = 1$.

É fácil verificar que $x = 0$ é uma solução para

$$f(x) \equiv 0 \ (mod\, 2), \tag{3.15}$$

assim,

$$f(0) = 5.0^2 - 3.0 + 16 \equiv 0 \ (mod\, 2)$$

logo, $x \equiv 0 \ (mod\, 2)$ e pelo teorema 2.1 $x = 0 + 2t$ também é solução para todo $t \in \mathbb{Z}$, ou seja,

$$f(0 + 2t) \equiv 0 \ (mod\, 2).$$

De fato, pelo binômio de Newton constatamos que para $k = 2$, temos que

$$(0+2t)^2 = 0^2 + \binom{2}{1} 0^{2-1}(2t) + \binom{2}{2} 0^{2-2}(2t)^2.$$

Como $2t \equiv 0\ (mod\, 2)$ e aplicando os conceitos de congruência no segundo membro da equação acima, obtemos que

$$0^2 + 0 + 0 \equiv 0^2\ (mod\, p),$$

logo, por transitividade,

$$(0+2t)^2 \equiv 0^2.$$

Portanto,

$$f(0+2t) \equiv f(0) \equiv 0\ (mod\, p),$$

ou seja, $0+2t$ também é solução de 3.15.

3° Passo - Queremos agora determinar $t \in \mathbb{Z}$ tal que $0+2t$ seja uma solução da equação

$$f(0+2t) \equiv 0\ (mod\, 2^2). \tag{3.16}$$

4° Passo/item *i* **-** vamos utilizar o desenvolvimento de Taylor de $f(x)$ no ponto $x = 0$ para encontrar o valor de t. Assim,

$$f(x) = f(0) + f'(0)(x-0) + \frac{f''(0)}{2!}(x-0)^2 + \ldots + \frac{f^{(k)}(0)}{k!}(x-0)^k.$$

4° Passo/item *ii* **-** Substituindo $x = 0+2t$ obtemos,

$$f(0+2t) = f(0) + f'(0)(0+2t-0) + \frac{f''(0)}{2!}(0+2t-0)^2 + \ldots + \frac{f^{(k)}(0)}{k!}(0+2t-0)^k.$$

ou ainda,

$$f(0+2t) = f(0) + f'(0)(2t) + \frac{f''(0)}{2!}(2t)^2 + \ldots + \frac{f^{(k)}(0)}{k!}(2t)^k,$$

distribuindo a potência, temos

$$f(0+2t) = f(0) + f^{'}(0)(2t) + \frac{f^{''}(0)}{2!}(2^2t^2) + \ldots + \frac{f^{(k)}(0)}{k!}(2^kt^k),$$

utilizando o conceito de congruências, obtemos

$$f(0+2t) \equiv f(0) + f^{'}(0)(2t) + \frac{f^{''}(0)}{2!}.0.t^2 + \ldots + \frac{f^{(k)}(0)}{k!}.0.t^k \equiv 0\ (mod\, 2^2).$$

Encontramos então, a seguinte congruência,

$$f(0+2t) \equiv f(0) + f^{'}(0)2t \equiv 0\ (mod\, 2^2), \tag{3.17}$$

pois, no desenvolvimento de $f(0+2t)$ acima, todas as potências de p, a partir da terceira parcela desta soma, são maiores ou iguais que a potência do módulo 2^2, logo são divisíveis por ele.

Tome

$$f(0)+f'(0)2t \equiv 0 \ (mod\, 2^2).$$

Como $f(0) \equiv 0 \ (mod\, 2)$, ou seja, $p|f(0)$ concluímos que $\frac{f(0)}{2} \in \mathbb{Z}$, e pelo teorema 1.9 item (2), obtemos

$$f'(0)2t \equiv -\frac{f(0)}{2} \ (mod\, 2^2).$$

Logo, observe que além de $f(0) = 16$ ser divisível por 2, os inteiros $f'(0)2t$ e 2^2 também são. Assim, utilizando o teorema 1.8 item(3) (passamos para o proxímo passo).

4° Passo/item *iii*- Encontramos a equação de congruência linear

$$f'(0)t \equiv -\frac{f(0)}{2} \ (mod\, 2). \tag{3.18}$$

Já sabemos que $f(0) = 16$, encontrando a derivada de $f(x)$ no ponto $x = 0$ temos $f'(0) = 10.0 - 3 = -3$, substituindo estes valores na equação 3.18 obtemos

$$-3t \equiv -8 \ (mod\, 2)$$

e pelo o exemplo 1.21 obtemos a equação

$$3t \equiv 8 \ (mod\, 2)$$

mas, $8 \equiv 0 \ (mod\, 2)$ logo,

$$3t \equiv 0 \ (mod\, 2)$$

$$3.t \equiv 3.0 \ (mod\, 2)$$

ou seja, por ser o $mdc(3,2) = 1$:

$$t \equiv 0 \ (mod\, 2).$$

Contudo, a definição 1.7 nos diz que $\exists t_1 \in \mathbb{Z}$ tal que $t = 0 + 2t_1$. Como $x = 0 + 2t$ colocamos $x = 0+2(0+2t_1) = 0+4t_1$ que também é uma solução para

$$f(0+4t_1) \equiv 0 \ (mod\, 2^2).$$

Observação: Fizemos, até aqui, todos os passos do Algoritmo para encontrarmos uma solução para $f(x) \equiv 0 \ (mod\, 2^2)$.

Mas, como o nosso objetivo é encontrarmos uma solução para

$$f(x) \equiv 0 \ (mod\, 2^3).$$

vamos realizar o mesmo procedimento a partir do **3º Passo**.

3° Passo - Tentaremos obter $t_1 \in \mathbb{Z}$ tal que

$$f(0+4t_1) \equiv 0 \ (mod\, 2^3).$$

4° Passo/item *i* **-** Em seguida, realizamos o desenvolvimento de Taylor de $f(x)$ no ponto $x = 0$. Logo,

$$f(x) = f(0) + f'(0)(x-0) + \frac{f''(0)}{2!}(x-0)^2 + \ldots + \frac{f^{(k)}(0)}{k!}(x-0)^k.$$

4° Passo/item *ii* **-** Substituindo $x = 0+4t_1$ no desenvolvimento de Taylor acima e aplicando o módulo, obtemos a congruência

$$f(0) + f'(0)4t_1 \equiv 0 \ (mod\, 2^3)$$

observe porém, que $f(0) \equiv 0 \ (mod\, 2^2)$ e pela definição de congruência $\frac{f(0)}{2^2} \in \mathbb{Z}$ onde, segundo o teorema 1.9 item (2) obtemos a equação

$$f'(0)4t_1 \equiv -\frac{f(0)}{4} \ (mod\, 2^3).$$

4° Passo/item *iii* **-** Pelo teorema 1.8 item 3, encontramos a equação de congruência linear

$$f'(0)t_1 \equiv -\frac{f(0)}{4} \ (mod\, 2).$$

Como $f(0) = 16$ e $f'(0) = -3$, obtemos a seguinte congruência

$$-3t_1 \equiv -4 \ (mod\, 2)$$

ou, pelo teorema 1.9 item(2) escrevemos a congruência equivalente

$$3t_1 \equiv 4 \ (mod\, 2).$$

Por ser o $mdc\,(3,2) = 1$ esta equação admite uma única solução, que em uma computação simples, verificamos

$$t_1 \equiv 0 \ (mod\, 2).$$

Tomando $t_1 = 0$ encontramos $x = 0+4t_1 = 0+4.0 = 0$, ou seja,

$$x \equiv 0 \ (mod\, 8)$$

é uma raiz de

$$5x^2 - 3x + 16 \equiv 0 \ (mod\, 8).$$

O que faremos a seguir é considerarmos que $m = p_1^{\alpha_1}, p_2^{\alpha_2}$, onde os $p_i^{'}s$ são primos distintos e $\alpha_i > 0$ para $i = 1,2$.

Sendo assim, a proposta é a de que precisamos encontrar soluções para

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (mod\, m)$$

com $m = p_1^{\alpha_1}, p_2^{\alpha_2}$. Contudo, obter soluções para a equação acima é equivalente a encontrar soluções para o sistema

$$\begin{cases} f(x) \equiv 0 \quad (mod\, p_1^{\alpha_1}) \\ f(x) \equiv 0 \quad (mod\, p_2^{\alpha_2}). \end{cases}$$

Observe que já resolvemos o caso, para o qual, $m_1 = p_1^{\alpha_1}$. Logo, uma solução para a primeira equação do sistema acima é $x = k_1$.[3]

Agora, queremos tentar obter soluções para $f(x)$, no caso em que, $m_2 = p_2^{\alpha_2}$.
Realizando o procedimento análogo a $f(x) \equiv 0 (mod\, p^{\alpha})$ com $\alpha = 3$, obtemos uma solução $x = k_2$ e concluímos que $x \equiv k_2 (mod\, p_2^{\alpha_2})$ é raiz de

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (mod\, p_2^{\alpha_2}).$$

Determinada as soluções para cada uma das equações acima módulo $m_1 = p_1^{\alpha_1}$, $m_2 = p_2^{\alpha_2}$, respectivamente, partiremos em busca de encontrar uma solução para o sistema

$$\begin{cases} x \equiv k_1 \quad (mod\, p_1^{\alpha_1}) \\ x \equiv k_2 \quad (mod\, p_2^{\alpha_2}) \end{cases} \tag{3.19}$$

o qual, pelo teorema Chinês do Resto (teorema 2.4), possui uma única solução x_0 módulo $m = p_1^{\alpha_1}.p_2^{\alpha_2}$, com $1 \leq x_0 < m$ e $p_1^{\alpha_1}$, $p_2^{\alpha_2}$ primos relativos.

Obtida a solução do sistema 3.19, vimos que

$$\begin{cases} x \equiv x_0 \quad (mod\, p_1^{\alpha_1}) \\ x \equiv x_0 \quad (mod\, p_2^{\alpha_2}). \end{cases}$$

Portanto, $x \equiv x_0 \ (mod\, m)$ é solução para a equação

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \ (mod\, m), \quad m = p_1^{\alpha_1} \cdot p_2^{\alpha_2}.$$

O que fizemos até aqui foi mostrar que, dado um polinômio de grau n e $m = p_1^{\alpha_1}.p_2^{\alpha_2}$ um módulo inteiro composto, podemos decompó-lo em fatores primos, os quais, apresentarão potências para cada p primo, fator de m.

[3] Algoritmo desenvolvido para $f(x) \equiv 0 \ (mod\, p^{\alpha})$

Exemplo 3.2. *Vamos obter uma solução para*

$$f(x) = x^3 - 4x^2 + 5x - 6 \equiv 0 \ (mod\, 36).$$

Solução: Como já vimos anteriormente, determinar uma solução para esta equação módulo $m = 2^2.3^2$ equivale a encontar uma solução para o sistema

$$\begin{cases} f(x) \equiv 0 \quad (mod\, 2^2) \\ f(x) \equiv 0 \quad (mod\, 3^2). \end{cases}$$

Sendo assim, vamos utilizar para cada potência de m os passos descritos no Algoritmo.

1° Passo - Como vimos, $m = 2^2 \cdot 3^2$. Tome inicialmente $m_1 = 2^2$;

2° Passo - Encontre a solução para $\alpha = 1$.

É fácil verificar que $f(0) = 0^3 - 4.0^2 + 5.0 - 6 \equiv 0 \ (mod\, 2)$, ou seja, $x \equiv 0 \ (mod\, 2)$ é uma solução módulo 2. Assim, pelo teorema 2.1 $x = 0 + 2t$, também é solução para todo $t \in \mathbb{Z}$, ou seja,

$$f(0 + 2t) \equiv 0 \ (mod\, 2).$$

Observe que utilizando o binômio de Newton constatamos que

$$f(0 + 2t) \equiv f(0) \equiv 0 \ (mod\, 2).$$

3° Passo - Precisamos determinar $t \in \mathbb{Z}$ tal que $x = 0 + 2t$ seja solução para $f(x) \equiv 0 \ (mod\, 2^2)$.

4° Passo/item *i* **-** [4]Utilizamos o desenvolvimento de Taylor de $f(x)$ na vizinhança de um ponto $x = 0$.

4° Passo/item *ii* **-** Desenvolvemos Taylor para $f(0 + 2t) \equiv 0 \ (mod\, 2^2)$ e aplicamos o módulo.

$$f(0 + 2t) \equiv f(0) + f'(0)2t \equiv 0 \ (mod\, 2^2).$$

Considere apenas o segundo membro da congruência

$$f(0) + f'(0)2t \equiv 0 \ (mod\, 2^2).$$

4° Passo/item *iii* **-** Como $f(0) \equiv 0 \ (mod\, 2)$, concluímos pela definição 1.7 que $\dfrac{f(0)}{2} \in \mathbb{Z}$, e pelo teorema 1.9 item(2) obtemos,

$$f'(0)2t \equiv -\frac{f(0)}{2} \ (mod\, 2^2).$$

[4] Procedimento realizado na demonstração do Algoritmo, onde consideramos $m = p_\alpha$

Logo, observe que além de $f(0) = -6$ ser divisível por 2, os inteiros $f'(0)2t$ e 2^2 também são. Assim, pelo teorema 1.8 item (3), encontramos a equação de congruência linear

$$f'(0)t \equiv -\frac{f(0)}{2} \ (mod\, 2). \tag{3.20}$$

Encontrando a derivada de $f(x)$ no ponto $x = 0$ temos $f'(0) = 3.0^2 - 8.0 + 5 = 5$ e substituindo nesta equação, obtemos

$$5t \equiv 3 \ (mod\, 2).$$

Logo, em uma computação simples verificamos que

$$t \equiv 1 \ (mod\, 2).$$

Tomando $t = 1$ encontramos $x = 0 + 2t = 0 + 2.1 = 2$, ou seja, $x \equiv 2 \ (mod\, 4)$ é raiz de

$$x^3 - 4x^2 + 5x - 6 \equiv 0 \ (mod\, 4).$$

Nosso interesse agora é determinar uma solução para

$$f(x) \equiv 0 \ (mod\, 3^2).$$

Sendo assim, vamos realizar o procedimento análogo ao de

$$f(x) \equiv 0 \ (mod\, 2^2).$$

1° Passo - Inicialmente, consideramos o módulo $m_2 = 3^2$.
2° Passo - Precisamos encontrar uma solução para $\alpha = 1$.
Primeiramente computamos que

$$f(0) = 0^3 - 4.0^2 + 5.0 - 6 \equiv 0 \ (mod\, 3),$$

ou seja, $x \equiv 0 \ (mod\, 3)$ é a única solução incongruente módulo 3. Logo, pelo teorema 2.1 $x = 0 + 3t$ e utilizando o binômio de Newton verificamos que

$$f(0 + 3t) \equiv f(0) \equiv 0 \ (mod\, 3)$$

ou seja, $0 + 3t$ também é solução de $f(x) \equiv 0 \ (mod\, 3)$.

3° Passo - Vamos determinar $t \in \mathbb{Z}$ tal que

$$f(0 + 3t) \equiv 0 \ (mod\, 3^2).$$

4° Passo/item *i* **-** Utilizamos o desenvolvimento de Taylor de $f(x)$ no ponto $x = 0$.

4° Passo/item *ii* **-** Substituimos $x = 0+3t$ no desenvolvimento de Taylor e a partir dos conceitos de congruência, aplicamos o módulo 3^2,

$$f(0+3t) \equiv f(0) + f'(0)3t \equiv 0 \ (mod\, 3^2).$$

Logo,

$$f(0) + f'(0)3t \equiv 0 \ (mod\, 3^2).$$

Como $f(0) \equiv 0 \ (mod\, 3)$, temos pela definição 1.7 que $\dfrac{f(0)}{3} \in \mathbb{Z}$, e pelo teorema 1.9 item(2) obtemos,

$$f'(0)3t \equiv -\frac{f(0)}{3} \ (mod\, 3^2).$$

Logo, observe que além de $f(0) = -6$ ser divisível por 3, os inteiros $f'(0)3t$ e 3^2 também são. Assim, pelo teorema 1.8 item (3), podemos dividir toda a congruência por uma constante, que no nosso caso é 3.

4° Passo/item *iii* **-** Encontramos a equação de congruência linear

$$f'(0)t \equiv -\frac{f(0)}{3} \ (mod\, 3). \tag{3.21}$$

Encontrando a derivada de $f(x)$ no ponto $x = 0$ temos, $f'(0) = 3.0^2 - 8.0 + 5 = 5$ e substituindo na equação, obtemos

$$5t \equiv 3 \ (mod\, 3).$$

Logo, verificamos que

$$t \equiv 1 \ (mod\, 2).$$

Tomando $t = 1$ encontramos $x = 0+3t = 0+3.1 = 3$, ou seja, $x \equiv 3 \ (mod\, 9)$ é raiz de

$$x^3 - 4x^2 + 5x - 6 \equiv 0 \ (mod\, 9).$$

Terminado o procedimeto para cada um dos módulos $m_1 = 2^2$ e $m_2 = 3^2$ encontramos o sistema

$$\begin{cases} x \equiv 2 \quad (mod\, 4) \\ x \equiv 3 \quad (mod\, 9). \end{cases}$$

A partir da daqui, vamos utilizar o teorema 2.4 (Chinês do Resto).

Observe que no sistema acima $m_1 = 4$ e $m_2 = 9$ e que o $mdc(4,9) = 1$, logo o sistema admite solução única módulo $m = 4 \cdot 9 = 36$.

Temos aqui

$$M_1 = \frac{m}{m_1} = \frac{36}{4} = 9 \quad \text{e} \quad M_2 = \frac{m}{m_2} = \frac{36}{9} = 4.$$

Daí, as congruências lineares

$$\begin{array}{rcccl} & M_1x & \equiv & 1 \quad (mod\, m_1) & \Longrightarrow \\ \Longrightarrow & 9x & \equiv & 1 \quad (mod\, 4) & \Longrightarrow \quad x = 1 \end{array}$$

e

$$\begin{array}{rcccl} & M_2x & \equiv & 1 \quad (mod\, m_2) & \Longrightarrow \\ \Longrightarrow & 4x & \equiv & 1 \quad (mod\, 9) & \Longrightarrow \quad x = 7. \end{array}$$

Portanto, o inteiro

$$X = 2.9.1 + 3.4.7 = 102,$$

como $102 \equiv -6\ (mod\, 36)$, segue que $X \equiv -6\ (mod\, 36)$ é a única solução do sistema de congruências lineares dado e, consequentemente

$$f(-6) = (-6)^3 - 4.(-6)^2 + 5.(-6) - 6 \equiv 0\ (mod\, 36)$$

como desejávamos.

Agora, considere $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ a forma padrão de m, onde os $p_i^{'}s$ são primos distintos e $\alpha_i > 0$ para todo $i \in \{1, \ldots, r\}$.

Observe, que encontrar soluções para a equação 3.1

$$f(x) \equiv 0\ (mod\, m)$$

equivale a encontrar soluções para o sistema

$$\begin{cases} f(x) \equiv 0 \quad (mod\, p_1^{\alpha_1}) \\ f(x) \equiv 0 \quad (mod\, p_2^{\alpha_2}) \\ \vdots \\ f(x) \equiv 0 \quad (mod\, p_r^{\alpha_r}), \end{cases} \tag{3.22}$$

onde $f(x) = a_n x^n + \ldots + a_1 x + a_0$, pois os primos $p_i^{'}s$ são todos distintos.

Vamos supor que seja possível obter soluções para a equação 3.1 no caso particular onde m é da forma $p_1^{\alpha_1}$.[5] Repare que podemos fazer o mesmo procedimeto para encontrarmos soluções, com m da forma $p_2^{\alpha_2}$ e, assim por diante, até chegarmos ao m da forma $p_r^{\alpha_r}$ desejado. Então, sejam $c_1, c_2, \ldots, c_r$ as respectivas soluções das r equações pertencentes ao sistema 3.22 acima. Logo,

[5] Procedimento realizado no Algoritmo para $m = p^{\alpha}$

$$\begin{cases} x \equiv c_1 & (mod\, p_1^{\alpha_1}) \\ x \equiv c_2 & (mod\, p_2^{\alpha_2}) \\ \vdots & \\ x \equiv c_r & (mod\, p_r^{\alpha_r}). \end{cases} \tag{3.23}$$

Ressaltamos que estas soluções são, em particular, de cada uma das equações que formam o sistema. Contudo, não necessariamente, são soluções do sistema.

Usando o teorema 2.4 (Chinês do Resto) podemos encontrar uma solução x_0 única módulo m para o sistema 3.23 acima, isto é

$$\begin{cases} x \equiv x_0 & (mod\, p_1^{\alpha_1}) \\ x \equiv x_0 & (mod\, p_2^{\alpha_2}) \\ \vdots & \\ x \equiv x_o & (mod\, p_r^{\alpha_r}). \end{cases}.$$

E agora é fácil verificar que x_0 é uma solução para o sistema 3.22, e portanto uma solução da equação 3.1, pois, para todo $i \in 1, \ldots, r$ temos que

$$f(x_0) \equiv f(c_i) \equiv 0\ (mod\, p_i^{\alpha_i}).$$

3.3 Aplicações

A seguir, iremos apresentar um exemplo de um polinômio de grau 4 com todas as suas raízes distintas em módulo.

Exemplo 3.3. *Seja* $f(x) = x^4 + 3x^3 - 8x^2 - 7x + 11 \equiv 0\ (mod\, 1500)$*, sabendo que* $1500 = 2^2.3.5^3$ *encontre todos os* $X \in \mathbb{Z}$ *de tal forma que satisfaça* $f(x)$*.*

Solução: Queremos saber as possíveis soluções de $f(x)$ módulo 1500.

De fato, $1500 = 2^2.3.5^3$ desta forma reescrevemos $f(x) \equiv 0\ (mod\, 1500)$, como um sistema de equações

$$\begin{cases} f(x) \equiv 0 & (mod\, 2^2) \\ f(x) \equiv 0 & (mod\, 3) \\ f(x) \equiv 0 & (mod\, 5^3). \end{cases}$$

Tomando a segunda equação do sistema, verificamos que para $x = 1$, temos

$$f(1) = 1^4 + 3.1^3 - 8.1^2 - 7.1 + 11 = 0$$

logo, $f(1) \equiv 0\ (mod\, 3)$.

Precisamos determinar soluções para $f(x) \equiv 0 \ (mod\, 4)$ e para $f(x) \equiv 0 \ (mod\, 125)$.

Então, fazendo o procedimento algorítmico para $f(x) \equiv 0 \ (mod\, 4)$ verificamos que $f(1) \equiv 0 \ (mod\, 2)$ é a única solução incongruente módulo 2, isto é, $x \equiv 1 \ (mod\, 2)$. Logo, pelo teorema 2.1, todas as demais soluções de $f(x)$ módulo 4 são da forma $x = 1 + 2t$, para todo $t \in \mathbb{Z}$. Sendo assim, tentaremos determinar um $t \in \mathbb{Z}$ de tal forma que

$$f(1+2t) \equiv 0 \ (mod\, 4).$$

Usando o desenvolvimento de Taylor de $f(x)$ com $x = 1 + 2t$, temos

$$f(1) + f^{'}(1)2t \equiv 0 \ (mod\, 4),$$

ou seja, pelo teorema 1.9 item(2)

$$f^{'}(1)2t \equiv -f(1) \ (mod\, 4).$$

Tendo em vista, que $f(1) \equiv 0 \ (mod\, 2)$, concluímos que $\dfrac{f(1)}{2} \in \mathbb{Z}$ e, consequentemente, pelo teorema 1.8 item(3), temos

$$f^{'}(1)t \equiv -\frac{f(1)}{2} \ (mod\, 2) \tag{3.24}$$

por serem os inteiros $f^{'}(1)2t$ e 4 divisíveis por 2.

Já sabemos que $f(1) = 0$, precisamos agora encontar a derivada de $f(x)$ no ponto $x = 1$

$$f^{'}(x) = 4x^3 + 9x^2 - 16x - 7 \qquad \text{e} \qquad f^{'}(1) = 4.1^3 + 9.1^2 - 16.1 - 7 = -10,$$

substituindo na congruência linear 3.24, obtemos

$$-10t \equiv 0 \ (mod\, 2)$$

observe que a congruência acima admite $d = 2$ soluções incongruentes módulo 2.

Tomando $t = 0$ obtemos $x = 1 + 2.0 = 1$, ou seja $x \equiv 1 \ (mod\, 4)$.

Tomando $t = 1$ obtemos $x = 1 + 2.1 = 3$, ou seja $x \equiv 3 \ (mod\, 4)$,

são raízes incongruentes de

$$x^4 + 3x^3 - 8x^2 - 7x + 11 \equiv 0 \ (mod\, 4).$$

Em seguida, iremos desenvolver o procedimento análogo para $f(x) \equiv 0 \ (mod\, 125)$.

Assim sendo, verificamos para $f(x) \equiv 0 \ (mod\, 5)$ existem 3 soluções incongruentes módulo 5. São elas

$$x \equiv 1 \ (mod\, 5), \qquad x \equiv 2 \ (mod\, 5) \qquad \text{e} \qquad x \equiv 3 \ (mod\, 5).$$

Tomando $x = 1+5t, \quad x = 2+5t \quad \text{e} \quad x = 3+5t$ tentaremos determinar $t \in \mathbb{Z}$ tal que

$$f(1+5t) \equiv 0 \ (mod\, 25), \tag{3.25}$$

$$f(2+5t) \equiv 0 \ (mod\, 25) \tag{3.26}$$

e

$$f(3+5t) \equiv 0 \ (mod\, 25). \tag{3.27}$$

Inicialmente, resolveremos a equação 3.25 e a partir do desenvolvimento de Taylor, reescrevemos a primeira das equações acima como

$$f(1) + f^{'}(1)5t \equiv 0 \ (mod\, 25),$$

isto é,

$$f^{'}(1)t \equiv -\frac{f(1)}{5} \ (mod\, 5).$$

Como já vimos, $f(1) = 0$ e $f^{'}(1) = -10$, ou seja,

$$-10t \equiv 0 \ (mod\, 5)$$

e já que o $mdc\,(-10, 5) = 5$ observe que esta equação possui exatamente 5 soluções incongruentes módulo 5, que são:

$t \equiv 0 \ (mod\, 5) \Longrightarrow t = 0+5t_1 \quad \text{e} \quad x = 1+5(0+5t_1) = 1+25t_1$
$t \equiv 1 \ (mod\, 5) \Longrightarrow t = 1+5t_1 \quad \text{e} \quad x = 1+5(1+5t_1) = 6+25t_1$
$t \equiv 2 \ (mod\, 5) \Longrightarrow t = 2+5t_1 \quad \text{e} \quad x = 1+5(2+5t_1) = 11+25t_1$
$t \equiv 3 \ (mod\, 5) \Longrightarrow t = 3+5t_1 \quad \text{e} \quad x = 1+5(3+5t_1) = 16+25t_1$
$t \equiv 4 \ (mod\, 5) \Longrightarrow t = 4+5t_1 \quad \text{e} \quad x = 1+5(4+5t_1) = 21+25t_1.$

Precisamos agora determinar $t_1 \in \mathbb{Z}$ tal que

$$f(1+25t_1) \equiv 0 \ (mod\, 125),$$

$$f(6+25t_1) \equiv 0 \ (mod\, 125),$$

$$f(11+25t_1) \equiv 0 \ (mod\, 125),$$

$$f(16+25t_1) \equiv 0 \ (mod\, 125)$$

e

$$f(21+25t_1) \equiv 0 \ (mod\, 125),$$

o que é equivalente (como já vimos no algoritmo) a encontrar as soluções das respectivas equações

$$f^{'}(1)t_1 \equiv -\frac{f(1)}{25} \ (mod\, 5), \tag{3.28}$$

$$f^{'}(6)t_1 \equiv -\frac{f(6)}{25} \ (mod\, 5), \tag{3.29}$$

$$f^{'}(11)t_1 \equiv -\frac{f(11)}{25} \ (mod\, 5), \tag{3.30}$$

$$f^{'}(16)t_1 \equiv -\frac{f(16)}{25} \ (mod\, 5) \tag{3.31}$$

e

$$f^{'}(21)t_1 \equiv -\frac{f(21)}{25} \ (mod\, 5). \tag{3.32}$$

Assim, teremos que resolver todas as equações, a fim de, obtermos as soluções incongruentes de $f(x) \equiv 0 \ (mod\, 125)$.

Iniciamos então, pela equação 3.28 obtendo

$$-10t_1 \equiv 0 \ (mod\, 5)$$

e imediatamente podemos perceber que esta, possui 5 soluções incongruentes módulo 5, quais sejam

$t_1 \equiv 0 \ (mod\, 5)$ tomando $t_1 = 0$ obtemos $x = 1 + 25.0 = 1$, ou seja $x \equiv 1 \ (mod\, 125)$.
$t_1 \equiv 1 \ (mod\, 5)$ tomando $t_1 = 1$ obtemos $x = 1 + 25.1 = 26$, ou seja $x \equiv 26 \ (mod\, 125)$,
$t_1 \equiv 2 \ (mod\, 5)$ tomando $t_1 = 2$ obtemos $x = 1 + 25.2 = 51$, ou seja $x \equiv 51 \ (mod\, 125)$,
$t_1 \equiv 3 \ (mod\, 5)$ tomando $t_1 = 3$ obtemos $x = 1 + 25.3 = 76$, ou seja $x \equiv 76 \ (mod\, 125)$,
$t_1 \equiv 4 \ (mod\, 5)$ tomando $t_1 = 4$ obtemos $x = 1 + 25.4 = 101$, ou seja $x \equiv 101 \ (mod\, 125)$.

Consecutivamente, determinaremos as soluções da equação 3.29, para tanto, precisamos encontrar

$$f(6) = 6^4 + 3.6^3 - 8.6^2 - 7.6 + 11 = 1625 \qquad \text{e} \qquad f^{'}(6) = 4.6^3 + 9.6^2 - 16.6 - 7 = 1085$$

e reescrever 3.29 como

$$1085t_1 \equiv -65 \ (mod\, 5),$$

ou seja, por ser o $mdc\,(1085, 5) = 5$ e $5 | -65$ a congruência linear acima admite 5 soluções incongruentes módulo 5. Logo,
para

$t_1 \equiv 0\ (mod\, 5)$ tomamos $t_1 = 0$ e obtemos $x = 6 + 25.0 = 6$, ou seja, $x \equiv 6\ (mod\, 125)$,
$t_1 \equiv 1\ (mod\, 5)$ tomamos $t_1 = 1$ e obtemos $x = 6 + 25.1 = 31$, ou seja, $x \equiv 31\ (mod\, 125)$,
$t_1 \equiv 2\ (mod\, 5)$ tomamos $t_1 = 2$ e obtemos $x = 6 + 25.2 = 56$, ou seja, $x \equiv 56\ (mod\, 125)$,
$t_1 \equiv 3\ (mod\, 5)$ tomamos $t_1 = 3$ e obtemos $x = 6 + 25.3 = 81$, ou seja, $x \equiv 81\ (mod\, 125)$,
$t_1 \equiv 4\ (mod\, 5)$ tomamos $t_1 = 4$ e obtemos $x = 6 + 25.4 = 106$, ou seja, $x \equiv 106\ (mod\, 125)$.

Agora, tomamos a equação 3.30 e determinamos

$$f(11) = 11^4 + 3.11^3 - 8.11^2 - 7.11 + 11 = 17600$$

e

$$f^{'}(11) = 4.11^3 + 9.11^2 - 16.11 - 7 = 6230$$

obtemos a equação

$$6230t_1 \equiv -704\ (mod\, 5),$$

observe que o $mdc\,(6230, 5) = 5$ e 5 não divide -704, o que nos leva a concluir que a congruência linear dada não admite solução módulo 5.

Em seguida, escrevemos a equação 3.31 e encontramos

$$f(16) = 16^4 + 3.16^3 - 8.16^2 - 7.16 + 11 = 75675$$

e

$$f^{'}(16) = 4.16^3 + 9.16^2 - 16.16 - 7 = 18425$$

escrevemos a equação

$$18425t_1 \equiv -3027\ (mod\, 5),$$

como o $mdc\,(18425, 5) = 5$ e não divide -3027, a equação acima não admite solução módulo 5.

Finalmente, da equação 3.32 obtemos

$$f(21) = 21^4 + 3.21^3 - 8.21^2 - 7.21 + 11 = 218600$$

e

$$f^{'}(21) = 4.21^3 + 9.21^2 - 16.21 - 7 = 40670$$

encontramos

$$40670t_1 \equiv -8744\ (mod\, 5),$$

como já vimos, a equação de congruêcia linear acima não possui solução, pois, o $mdc\,(40670, 5) = 5$ e 5 não divide -8744.

Retornando à equação 3.26, podemos reescrevê-la usando o desenvolvimento de Taylor de $f(x)$ de tal forma que

$$f(2) + f^{'}(2)5t \equiv 0\ (mod\, 25)$$

ou ainda,

$$f^{'}(2)t \equiv -\frac{f(2)}{5} \ (mod\, 5)$$

como

$$f(2) = 2^4 + 3.2^3 - 8.2^2 - 7.2 + 11 = 5 \qquad \text{e} \qquad f^{'}(2) = 4.2^3 + 9.2^2 - 16.2 - 7 = 29$$

podemos escrever a equação

$$29t \equiv -1 \ (mod\, 5)$$

e já que 29 e 5 são primos entre si, a equação admite solução única módulo 5, qual seja,

$$t \equiv 1 \ (mod\, 5).$$

Colocando $t = 1 + 5t_1$ obtemos $x = 2 + 5t = 2 + 5(1 + 5t_1) = 7 + 25t_1$, e tentaremos obter $t_1 \in \mathbb{Z}$ tal que

$$f(7 + 25t_1) \equiv 0 \ (mod\, 125),$$

donde obtemos a equação

$$f^{'}(7)t_1 \equiv -\frac{f(7)}{25} \ (mod\, 5),$$

determinando $f(7) = 7^4 + 3.7^3 - 8.7^2 - 7.7 + 11 = 3000$ e $f^{'}(7) = 4.7^3 + 9.7^2 - 16.7 - 7 = 1694$, escrevemos a congruência linear

$$1694t_1 \equiv -120 \ (mod\, 5)$$

e como o $mdc\,(1694, 5) = 1$ a equação admite solução única módulo 5, qual seja,

$$t_1 \equiv 0 \ (mod\, 5).$$

Tomando $t_1 = 0$ obtemos $x = 7 + 25.0 = 7$, ou seja, $x \equiv 7 \ (mod\, 125)$.

Por fim, vamos calcular a equação 3.27, logo, podemos reescrever esta equação utilizando o desenvolvimento de Taylor de $f(x)$, obtendo a congruência

$$f(3) + f^{'}(3)5t \equiv 0 \ (mod\, 5)$$

ou,

$$f^{'}(3)t \equiv -\frac{f(3)}{5} \ (mod\, 5)$$

donde determinamos

$$f(3) = 3^4 + 3.3^3 - 8.3^2 - 7.3 + 11 = 80 \qquad \text{e} \qquad f^{'}(3) = 4.3^3 + 9.3^2 - 16.3 - 7 = 134$$

de tal forma, que escrevemos a equação

$$134t \equiv -16 \ (mod\, 5).$$

Como podemos observar, o $mdc\,(134, 5) = 1$, logo, a congruência linear dada possui solução única módulo 5, qual seja

$$t \equiv 1 \ (mod\, 5).$$

Colocando $t = 1+5t_1$ obtemos $x = 3+5t = 3+5(1+5t_1) = 8+25t_1$ e tentaremos obter $t_1 \in \mathbb{Z}$ tal que

$$f(8+25t_1) \equiv 0 \ (mod\, 125)$$

o que é equivalente a escrever a equação

$$f^{'}(8)t_1 \equiv -\frac{f(8)}{25} \ (mod\, 5),$$

como

$$f(8) = 8^4 + 3.8^3 - 8.8^2 - 7.8 + 11 = 5075 \qquad \text{e} \qquad f^{'}(8) = 4.8^3 + 9.8^2 - 16.8 - 7 = 2489$$

obtemos a equação

$$2489t_1 \equiv -203 \ (mod\, 5),$$

podemos observar que a equação de congruência acima admite solução única, logo

$$t_1 \equiv 3 \ (mod\, 5).$$

Tomando $t_1 = 3$ obtemos $x = 8+25t_1 = 8+25.3 = 83$, ou seja $x \equiv 83 \ (mod\, 125)$. Logo, concluímos que $x \equiv 1, 6, 7, 26, 31, 51, 56, 76, 81, 83, 101, 106 \ (mod\, 125)$ são raízes de

$$x^4 + 3x^3 - 8x^2 - 7x + 11 \equiv 0 \ (mod\, 125).$$

Neste ponto precisamos encontrar uma solução para cada um dos 24 sistemas

$$(1)\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 1 & (mod\, 125) \end{cases} \quad (2)\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 6 & (mod\, 125) \end{cases} \quad (3)\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 7 & (mod\, 125) \end{cases}$$

$$(4)\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 26 & (mod\, 125) \end{cases} \quad (5)\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 31 & (mod\, 125) \end{cases} \quad (6)\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 51 & (mod\, 125) \end{cases}$$

$$(7)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 1 & (mod\,4) \\ x \equiv 56 & (mod\,125) \end{cases} \quad (8)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 1 & (mod\,4) \\ x \equiv 76 & (mod\,125) \end{cases} \quad (9)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 1 & (mod\,4) \\ x \equiv 81 & (mod\,125) \end{cases}$$

$$(10)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 1 & (mod\,4) \\ x \equiv 83 & (mod\,125) \end{cases} \quad (11)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 1 & (mod\,4) \\ x \equiv 101 & (mod\,125) \end{cases} \quad (12)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 1 & (mod\,4) \\ x \equiv 106 & (mod\,125) \end{cases}$$

$$(13)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 1 & (mod\,125) \end{cases} \quad (14)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 6 & (mod\,125) \end{cases} \quad (15)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 7 & (mod\,125) \end{cases}$$

$$(16)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 26 & (mod\,125) \end{cases} \quad (17)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 31 & (mod\,125) \end{cases} \quad (18)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 51 & (mod\,125) \end{cases}$$

$$(19)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 56 & (mod\,125) \end{cases} \quad (20)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 76 & (mod\,125) \end{cases} \quad (21)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 81 & (mod\,125) \end{cases}$$

$$(22)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 83 & (mod\,125) \end{cases} \quad (23)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 101 & (mod\,125) \end{cases} \quad (24)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 106 & (mod\,125) \end{cases}$$

e para isto utilizamos o teorema 2.4 do Resto Chinês em cada um dos sistemas apresentados. Temos aqui:

$$(1)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 1 & (mod\,4) \\ x \equiv 1 & (mod\,125) \end{cases}.$$

Como o $mdc\,(3,4) = mdc\,(3,125) = mdc\,(4,125) = 1$ o sistema dado admite solução única módulo $m = 3.4.125 = 1500$.

Logo,

$$M_1 = \frac{m}{m_1} = \frac{1500}{3} = 500, \qquad M_2 = \frac{m}{m_2} = \frac{1500}{4} = 375 \qquad \text{e} \qquad M_3 = \frac{m}{m_3} = \frac{1500}{125} = 12.$$

Calculamos então as congruências lineares

$$
\begin{array}{lcll}
M_1x_1 & \equiv & 1 & (mod\, m_1) \\
500x_1 & \equiv & 1 & (mod\, 3) \quad \text{como } 1 \equiv -5\ (mod\, 3) \\
500x_1 & \equiv & -5 & (mod\, 3) \\
5.100x_1 & \equiv & 5.-1 & (mod\, 3) \quad \text{como, o } mdc\,(5,3) = 1 \\
100x_1 & \equiv & -1 & (mod\, 3) \quad \text{como, } -1 \equiv -25\ (mod\, 3) \\
100x_1 & \equiv & -25 & (mod\, 3) \\
25.4x_1 & \equiv & 25.-1 & (mod\, 3) \quad \text{por ser o } mdc\,(25,3) = 1 \\
4x_1 & \equiv & -1 & (mod\, 3) \quad \text{como, } -1 \equiv -4\ (mod\, 3) \\
4x_1 & \equiv & -4 & (mod\, 3) \\
4.x_1 & \equiv & 4.(-1) & (mod\, 3) \quad \text{como, o } mdc\,(4,3) = 1 \\
x_1 & \equiv & -1 & (mod\, 3),
\end{array}
$$

e

$$
\begin{array}{lcll}
M_2x_2 & \equiv & 1 & (mod\, m_2) \\
375x_2 & \equiv & 1 & (mod\, 4) \quad \text{como } 1 \equiv 25\ (mod\, 4) \\
375x_2 & \equiv & 25 & (mod\, 4) \\
25.15.x_2 & \equiv & 25.1 & (mod\, 4) \quad \text{como, o } mdc\,(25,4) = 1 \\
15x_2 & \equiv & 1 & (mod\, 4) \quad \text{como } 1 \equiv 5\ (mod\, 4) \\
15x_2 & \equiv & 5 & (mod\, 4) \\
5.3x_2 & \equiv & 5.1 & (mod\, 4) \quad \text{por ser o } mdc\,(5,4) = 1 \\
3x_2 & \equiv & 1 & (mod\, 4) \quad \text{como } 1 \equiv -3\ (mod\, 4) \\
3x_2 & \equiv & -3 & (mod\, 4) \\
3.x_2 & \equiv & 3.-1 & (mod\, 4) \quad \text{por ser o } mdc\,(3,4) = 1 \\
x_2 & \equiv & -1 & (mod\, 4)
\end{array}
$$

e

$$
\begin{array}{lcll}
M_3x_3 & \equiv & 1 & (mod\, m_3) \\
12x_3 & \equiv & 1 & (mod\, 125) \quad \text{como } 1 \equiv -124\ (mod\, 125) \\
12x_3 & \equiv & -124 & (mod\, 125) \\
4.3x_3 & \equiv & 4.-31 & (mod\, 125) \quad \text{por ser o } mdc\,(4,125) = 1 \\
3x_3 & \equiv & -31 & (mod\, 125) \quad \text{como } -31 \equiv 219\ (mod\, 125) \\
3x_3 & \equiv & 219 & (mod\, 125) \\
3.x_3 & \equiv & 3.73 & (mod\, 125) \quad \text{por ser o } mdc\,(3,125) = 1 \\
x_3 & \equiv & 73 & (mod\, 125).
\end{array}
$$

Portanto, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 1.12.73 = 1$$

donde segue que $X \equiv 1\ (mod\, 1500)$ é a única solução do sistema dado e, consequentemente

$$f(1) = 1^4 + 3.1^3 - 8.1^2 - 7.1 + 11 \equiv 0\ (mod\, 1500).$$

Fazendo o mesmo para o sistema $(2)\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 6 \pmod{125} \end{cases}$, temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$.

As congruências lineares

$$\begin{aligned} & 500x_1 \equiv 1 \pmod 3 \implies \\ \implies & x_1 \equiv -1 \pmod 3 \\ & 375x_2 \equiv 1 \pmod 4 \implies \\ \implies & x_2 \equiv -1 \pmod 4. \end{aligned}$$

e

$$\begin{aligned} & 12x_3 \equiv 1 \pmod{125} \implies \\ \implies & x_3 \equiv 73 \pmod{125} \end{aligned}$$

Portanto, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 6.12.73 = 4381.$$

Como $4381 \equiv -119 \pmod{1500}$ segue que $X \equiv -119 \pmod{1500}$ é solução única do sistema apresentado e, consequentemente,

$$f(-119) = (-119)^4 + 3.(-119)^3 - 8.(-119)^2 - 7.(-119) + 11 \equiv 0 \pmod{1500}.$$

Para o sistema $(3)\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 7 \pmod{125} \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Portanto, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 7.12.73 = 5257$$

donde segue que $5257 \equiv 757 \pmod{1500}$, ou seja, $X \equiv 757 \pmod{1500}$ é a única solução deste sistema, e

$$f(757) = 757^4 + 3.757^3 - 8.757^2 - 7.757 + 11 \equiv 0 \pmod{1500}.$$

Fazendo procedimento análogo para $(4)\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 26 \pmod{125} \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Portanto, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 26.12.73 = 21901.$$

Como $21901 \equiv -599 \ (mod\, 1500)$ temos que $X \equiv -599 \ (mod\, 1500)$ é solução única deste sistema, logo é solução também de

$$f(-599) = (-599)^4 + 3.(-599)^3 - 8.(-599)^2 - 7.(-599) + 11 \equiv 0 \ (mod\, 1500).$$

Agora, faremos os mesmos passos para o sistema $(5)\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 31 & (mod\, 125) \end{cases}$ daí, temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.
Assim, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 31.12.73 = 26281$$

donde segue que $26281 \equiv -719 \ (mod\, 1500)$, ou seja, $X \equiv -719 \ (mod\, 1500)$ é solução única do sistema e, consequentemente,

$$f(-719) = (-719)^4 + 3.(-719)^3 - 8.(-719)^2 - 7.(-719) + 11 \equiv 0 \ (mod\, 1500).$$

Tomando o sistema $(6)\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 51 & (mod\, 125) \end{cases}$ obtemos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.
Assim, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 51.12.73 = 43801.$$

Como $43801 \equiv 301 \ (mod\, 1500)$ segue que $X \equiv 301 \ (mod\, 1500)$ é solução única deste sistema, e é também de

$$f(301) = 301^4 + 3.301^3 - 8.301^2 - 7.301 + 11 \equiv 0 \ (mod\, 1500).$$

Fazendo o procedimento para $(7)\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 56 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.
Logo, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 56.12.73 = 48181$$

donde segue que $48181 \equiv 181 \ (mod\, 1500)$, ou seja, $X \equiv 181 \ (mod\, 1500)$ é solução única deste sistema e, consequentemente,

$$f(181) = 181^4 + 3.181^3 - 8.181^2 - 7.181 + 11 \equiv 0 \ (mod\, 1500).$$

Para o sistema (8) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 76 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Portanto, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 76.12.73 = 65701.$$

Como $65701 \equiv -299\ (mod\, 1500)$ segue que $X \equiv -299\ (mod\, 1500)$ é solução única do sistema dado, e satisfaz

$$f(-299) = (-299)^4 + 3.(-299)^3 - 8.(-299)^2 - 7.(-299) + 11 \equiv 0\ (mod\, 1500).$$

Para o sistema (9) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 81 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Portanto, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 81.12.73 = 70081$$

donde segue que $70081 \equiv -419\ (mod\, 1500)$, ou seja, $X \equiv -419\ (mod\, 1500)$ é solução única do sistema de congruências lineares, e satisfaz

$$f(-419) = (-419)^4 + 3.(-419)^3 - 8.(-419)^2 - 7.(-419) + 11 \equiv 0\ (mod\, 1500).$$

Para o sistema (10) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 83 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Assim, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 83.12.73 = 71833.$$

Como $71833 \equiv -167\ (mod\, 1500)$ segue que $X \equiv -167\ (mod\, 1500)$ é a única solução do sistema dado, logo, é solução de

$$f(-167) = (-167)^4 + 3.(-167)^3 - 8.(-167)^2 - 7.(-167) + 11 \equiv 0\ (mod\, 1500).$$

Para o sistema (11) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 101 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Logo, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 101.12.73 = 87601$$

donde segue que $87601 \equiv 601\ (mod\, 1500)$, ou seja, $X \equiv 601\ (mod\, 1500)$ é solução única do sistema de congruências lineares, e satisfaz

$$f(601) = (601)^4 + 3.(601)^3 - 8.(601)^2 - 7.(601) + 11 \equiv 0\ (mod\, 1500).$$

Para o sistema (12) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 1 & (mod\, 4) \\ x \equiv 106 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Logo, o inteiro

$$X = 1.500.(-1) + 1.375.(-1) + 106.12.73 = 91981.$$

Como $91981 \equiv 481\ (mod\, 1500)$ segue que $X \equiv 481\ (mod\, 1500)$ é solução única deste sistema e, consequentemente

$$f(481) = (481)^4 + 3.(481)^3 - 8.(481)^2 - 7.(481) + 11 \equiv 0\ (mod\, 1500).$$

Para o sistema (13) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 3 & (mod\, 4) \\ x \equiv 1 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Assim, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 1.12.73 = -749$$

donde segue que $X \equiv -749$ é a única solução do sistema apresentado e, consequentemente, satisfaz

$$f(-749) = (-749)^4 + 3.(-749)^3 - 8.(-749)^2 - 7.(-749) + 11 \equiv 0\ (mod\, 1500).$$

Para o sistema (14) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 3 & (mod\, 4) \\ x \equiv 6 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Portanto, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 6.12.73 = 3631.$$

Como $3631 \equiv 631 \ (mod\, 1500)$ segue que $X \equiv 631 \ (mod\, 1500)$ é solução única do sistema de congruências lineares, e satisfaz

$$f(631) = (631)^4 + 3.(631)^3 - 8.(631)^2 - 7.(631) + 11 \equiv 0 \ (mod\, 1500).$$

Para o sistema (15) $\begin{cases} x \equiv 1 \quad (mod\, 3) \\ x \equiv 3 \quad (mod\, 4) \\ x \equiv 7 \quad (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Portanto, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 7.12.73 = 4507$$

donde segue que $4507 \equiv 7 \ (mod\, 1500)$, ou seja, $X \equiv 7 \ (mod\, 1500)$ é solução única do sistema, e satisfaz

$$f(7) = 7^4 + 3.7^3 - 8.7^2 - 7.7 + 11 \equiv 0 \ (mod\, 1500).$$

Para o sistema (16) $\begin{cases} x \equiv 1 \quad (mod\, 3) \\ x \equiv 3 \quad (mod\, 4) \\ x \equiv 26 \quad (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Logo, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 26.12.73 = 21151.$$

Como $21151 \equiv 151 \ (mod\, 1500)$ segue que $X \equiv 151 \ (mod\, 1500)$ é a única solução deste sistema, e satistaz

$$f(151) = 151^4 + 3.151^3 - 8.151^2 - 7.151 + 11 \equiv 0 \ (mod\, 1500).$$

Para o sistema (17) $\begin{cases} x \equiv 1 \quad (mod\, 3) \\ x \equiv 3 \quad (mod\, 4) \\ x \equiv 31 \quad (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Logo, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 31.12.73 = 25531$$

donde segue que $25531 \equiv 31 \ (mod\, 1500)$, ou seja, $X \equiv 31 \ (mod\, 1500)$ é solução única do sistema de congruências lineares, e consequentemente

$$f(31) = 31^4 + 3.31^3 - 8.31^2 - 7.31 + 11 \equiv 0 \ (mod\, 1500).$$

Para o sistema (18) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 3 & (mod\, 4) \\ x \equiv 51 & (mod\, 125) \end{cases}$ temos $x_1 = 500$, $x_2 = 375$ e $x_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Assim o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 51.12.73 = 43051.$$

Como $43051 \equiv -449 \ (mod\, 1500)$ segue que $X \equiv -449 \ (mod\, 1500)$ é a única solução do sistema e, consequentemente,

$$f(-449) = (-449)^4 + 3.(-449)^3 - 8.(-449)^2 - 7.(-449) + 11 \equiv 0 \ (mod\, 1500).$$

Para o sistema (19) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 3 & (mod\, 4) \\ x \equiv 56 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Assim, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 56.12.73 = 47431$$

donde segue que $47431 \equiv -569$ $(mod\, 1500$, ou seja, $X \equiv -569 \ (mod\, 1500)$ é solução única do sistema de congruências lineares dado, e consequentemente

$$f(-569) = (-569)^4 + 3.(-569)^3 - 8.(-569)^2 - 7.(-569) + 11 \equiv 0 \ (mod\, 1500).$$

Para o sistema (20) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 3 & (mod\, 4) \\ x \equiv 76 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Portanto, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 76.12.73 = 64951.$$

Como $64951 \equiv 451 \ (mod\, 1500)$ segue que $X \equiv 451 \ (mod\, 1500)$ é solução única deste sistema, e satisfaz

$$f(451) = (451)^4 + 3.(451)^3 - 8.(451)^2 - 7.(451) + 11 \equiv 0 \ (mod\, 1500).$$

Para o sistema (21) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 3 & (mod\, 4) \\ x \equiv 81 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Portanto, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 81.12.73 = 69331$$

donde segue que $69331 \equiv 331\ (mod\, 1500)$, ou seja, $X \equiv 331\ (mod\, 1500)$ é a única solução do sistema de congruências lineares, e satisfaz

$$f(331) = (331)^4 + 3.(331)^3 - 8.(331)^2 - 7.(331) + 11 \equiv 0\ (mod\, 1500).$$

Para o sistema (22) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 3 & (mod\, 4) \\ x \equiv 83 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Logo, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 83.12.73 = 71083.$$

Como $71083 \equiv 583\ (mod\, 1500)$ segue que $X \equiv 583\ (mod\, 1500)$ é a única solução deste sistema e, consequentemente, satisfaz

$$f(583) = (583)^4 + 3.(583)^3 - 8.(583)^2 - 7.(583) + 11 \equiv 0\ (mod\, 1500).$$

Para o sistema (23) $\begin{cases} x \equiv 1 & (mod\, 3) \\ x \equiv 3 & (mod\, 4) \\ x \equiv 101 & (mod\, 125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Logo, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 101.12.73 = 86851$$

donde segue que $86851 \equiv -149\ (mod\, 1500)$, ou seja, $X \equiv -149\ (mod\, 1500)$ é solução única do sistema apresentado e, consequentemente, satisfaz

$$f(-149) = (-149)^4 + 3.(-149)^3 - 8.(-149)^2 - 7.(-149) + 11 \equiv 0\ (mod\, 1500).$$

Para o sistema $(24)\begin{cases} x \equiv 1 & (mod\,3) \\ x \equiv 3 & (mod\,4) \\ x \equiv 106 & (mod\,125) \end{cases}$ temos $M_1 = 500$, $M_2 = 375$ e $M_3 = 12$, $x_1 = -1$, $x_2 = -1$ e $x_3 = 73$.

Portanto, o inteiro

$$X = 1.500.(-1) + 3.375.(-1) + 106.12.73 = 91231.$$

Como $91231 \equiv -269\ (mod\,1500)$ segue que $X \equiv -269\ (mod\,1500)$ é solução única do sistema de congruências lineares dado, e satisfaz

$$f(-269) = (-269)^4 + 3.(-269)^3 - 8.(-269)^2 - 7.(-269) + 11 \equiv 0\ (mod\,1500).$$

Logo, $x \equiv -749, -719, -599, -569, -449, -419, -299, -269, -167,, -149, -119, 1, 7, 31, 151, 181, 301, 331, 451, 481, 583, 601, 631, 757\ (mod\,1500)$
como desejávamos.

De posse do conhecimento do Algoritmo, vamos ilustrar o processo desenvolvido por ele, com outra aplicação em equações de congruência, desta vez, o nosso polinômio tem grau igual a 5 e módulo igual a $1875 = 3.5^4$.

Exemplo 3.4. *Obtenha uma solução para a equação*

$$f(x) = x^5 + x^4 - x^3 + 3x^2 - 12 \equiv 0\ (mod\,1875).$$

Inicialmente, decompomos o número $1875 = 3.5^4$ em fatores primos e reescrevemos a equação acima na forma de sistema

$$\begin{cases} f(x) \equiv 0 & (mod\,5^4) \\ f(x) \equiv 0 & (mod\,3). \end{cases}$$

Como já vimos nas equações anteriores, é possível estabelecer uma solução para $f(x) \equiv 0\ (mod\,3)$, então facilmente verificamos que $f(0) \equiv 0\ (mod\,3)$.

A preocupação agora é determinar uma solução para $f(x) \equiv 0\ (mod\,625)$. E não obstante as demais, seguiremos todo o procedimento descrito no algoritmo, determinando primeiramente soluções módulo 5.

Sendo assim, computamos que

$$f(2) = 2^5 + 2^4 - 2^3 + 3.2^2 - 12 = 40 \equiv 0\ (mod\,5)$$

é a única solução incongruente módulo 5. Tomando $x \equiv 2\ (mod\, 5)$ obtemos pelo teorema 2.1 $x = 2+5t$, observando que

$$f(2+5t) \equiv 0\ (mod\, 5)$$

tentaremos determinar $t \in \mathbb{Z}$ tal que

$$f(2+5t) \equiv 0\ (mod\, 25).$$

Utilizando o desenvolvimento de Taylor para $f(2+5t)$ temos

$$f(2) + f^{'}(2)5t \equiv 0\ (mod\, 25)$$

o que é equivalente pelo teorema 1.9 item(2) a encontrar as soluções da equação

$$f^{'}(2)5t \equiv -f(2)\ (mod\, 25).$$

Observe que $f^{'}(2)5t$, $f(2)$ e 25 são números inteiros divisíveis por 5, logo, pelo teorema 1.8 item(3)

$$f^{'}(2)t \equiv -\frac{f(2)}{5}\ (mod\, 5).$$

Veja que $f^{'}(2) = 5.2^4 + 4.2^3 - 3.2^2 + 6.2 = 112$ é a derivada de $f(x)$ no ponto $x = 2$. Assim, obtemos a congruência linear

$$112t \equiv -\frac{40}{5}\ (mod\, 5)$$

ou,

$$112t \equiv -8\ (mod\, 5). \tag{3.33}$$

Como o $mdc\,(112, 5) = 1$, a congruência 3.33 acima admite solução única módulo 5. Temos:

$$8.14t \equiv 8.(-1)\ (mod\, 5),$$

ou seja, por ser o $mdc\,(8, 5) = 1$:

$$14t \equiv -1\ (mod\, 5),$$

como $-1 \equiv 14\ (mod\, 5)$, temos:

$$14t \equiv 14\ (mod\, 5),$$

por ser o $mdc\,(14, 5) = 1$

$$t \equiv 1\ (mod\, 5).$$

Baseado na definição 1.7 de congruência, obtemos $t = 1+5t_1$ e $x = 2+5t = 2+5.(1+5t_1) = 7+25t_1$, para todo $t_1 \in \mathbb{Z}$. Agora, tentaremos obter $t_1 \in \mathbb{Z}$ tal que

$$f(7+25t_1) \equiv 0 \ (mod\, 125).$$

Reescrevendo $f(7+125t_1)$ a partir do desenvolvimento de Taylor para $f(x)$ com $x = 7$, temos

$$f(7)+f^{'}(7)25t_1 \equiv 0 \ (mod\, 125)$$

daqui, utilizamos os teoremas 1.9 item(2) e 1.8 item(3), respectivamente, obtemos

$$f^{'}(7)t_1 \equiv -\frac{f(7)}{25} \ (mod\, 5). \tag{3.34}$$

Precisamos agora encontrar $f(7)$ e $f^{'}(7)$, quais sejam

$$f(7) = 7^5+7^4-7^3+3.7^2-12 = 19000$$

e

$$f^{'}(7) = 5.7^4+4.7^3-3.7^2+6.7 = 13272,$$

substituindo na equação 3.34 temos

$$13272t_1 \equiv -\frac{19000}{25} \ (mod\, 5),$$

ou,

$$13272t_1 \equiv -760 \ (mod\, 5)$$

observe que 5 não divide 13272, logo, a congruência dada admite uma única solução

$$t_1 \equiv 0 \ (mod\, 5).$$

Colocando $t_1 = 0+5t_2$, obtemos $x = 7+25t_1 = 7+25.(0+5t_2) = 7+125t_2$, e tentaremos então obter $t_2 \in \mathbb{Z}$ tal que

$$f(7+125t_2) \equiv 0 \ (mod\, 625).$$

Então, usando Taylor temos

$$f(7)+f^{'}(7)125t_2 \equiv 0 \ (mod\, 625)$$

o que implica

$$f^{'}(7)t_2 \equiv -\frac{f(7)}{125} \ (mod\, 5)$$

ou,

$$13272t_2 \equiv -152 \ (mod\, 5)$$

ou ainda,

$$8.1659t_2 \equiv 8.(-19) \ (mod\, 5)$$

e pelo teorema 1.1, por ser o $mdc\,(8, 5) = 1$

$$1659t_2 \equiv -19 \ (mod\, 5),$$

observe que $-19 \equiv 6 \ (mod\, 5)$ logo, por transitividade

$$1659t_2 \equiv 6 \ (mod\, 5)$$

$$3.553t_2 \equiv 3.2 \ (mod\, 5)$$

ou seja, por ser o $mdc\,(3, 5) = 1$, (teorema 1.1) obtemos

$$553t_2 \equiv 2 \ (mod\, 5),$$

como $2 \equiv 182 \ (mod\, 5)$, temos

$$553t_2 \equiv 182 \ (mod\, 5)$$

$$7.79t_2 \equiv 7.26 \ (mod\, 5)$$

ou seja, por ser o $mdc\,(7, 5) = 1$

$$79t_2 \equiv 26 \ (mod\, 5)$$

isto é,

$$t_2 \equiv 4 \ (mod\, 5).$$

Tomando $t_2 = 4$ encontramos $x = 7 + 125.4 = 507$, ou seja, $x \equiv 507 \ (mod\, 625)$ é raiz de

$$x^5 + x^4 - x^3 + 3x^2 - 12 \equiv 0 \ (mod\, 625).$$

Desta forma precisamos encontrar uma solução para

$$\begin{cases} x \equiv 507 & (mod\, 625) \\ x \equiv 0 & (mod\, 3). \end{cases}$$

e para isto utilizamos o teorema do Resto Chinês.

Os módulos 625 e 3 das congruências do sistema obtido, são primos entre si, de modo que, o sistema possui uma única solução módulo $m = 625.3 = 1875$.

Temos aqui

$$M_1 = \frac{m}{m_1} = \frac{1875}{625} = 3 \qquad \text{e} \qquad M_2 = \frac{m}{m_2} = \frac{1875}{3} = 625.$$

Calculamos então as congruências lineares

$$\begin{array}{rrcll} & M_1 x_1 & \equiv & 1 \quad (mod\, m_1) & \Longrightarrow \\ \Longrightarrow & 3x_1 & \equiv & 1 \quad (mod\, 625) & \Longrightarrow \quad x_1 = 417 \end{array}$$

e

$$\begin{array}{rrcll} & M_2 x_2 & \equiv & 1 \quad (mod\, m_2) & \Longrightarrow \\ \Longrightarrow & 625x_2 & \equiv & 1 \quad (mod\, 3) & \Longrightarrow \quad x_2 = 1. \end{array}$$

Portanto, o inteiro

$$X = 507.3.417 + 0.625.1 = 634257.$$

Como $634257 \equiv 507\ (mod\, 1875)$, segue-se que $X \equiv 507\ (mod\, 1875)$ é a única solução do sistema de congruências lineares obtido e, consequentemente

$$f(507) = 507^5 + 507^4 - 507^3 + 3.507^2 - 12 \equiv 0\ (mod\, 1875),$$

logo,

$$f(507) \equiv 0\ (mod\, 1875).$$

como queríamos.

Conclusão

Algumas das questões relevantes para a teoria dos números foram abordadas neste trabalho, principalmente, as que estão relacionadas com a teoria das congruências que, dentro do universo da matemática pura, podem ser aplicadas em equações módulo um inteiro m positivo, ou seja, feita uma analogia do símbolo $\equiv$ usado nas congruências, com o símbolo $=$ usado nas equações convencionais, podemos encontrar soluções para equações, via congruência.

Sendo assim, preocupamo-nos em desenvolver uma pesquisa sobre a resolução de equações de congruência de grau maior que um, onde, inicialmente, apresentamos os resultados básicos, porém fundamentais para o desenvolvimento do tema em questão.

Todavia, concluímos que a partir da teoria das congruências, podemos resolver equações envolvendo um módulo m, quais sejam, os polinômios de grau um, que se configuram como equações de congruências lineares e os polinômios de grau maior que um, que são tidos também como as equações de congruências não-lineares.

Em suma, diante do que abordamos neste trabalho, esperamos contribuir para uma melhor compreensão, por parte do leitor, do algoritmo apresentado que é desenvolvido a partir da fórmula de Taylor. E assim, instigar nos leitores a curiosidade de encontrar soluções para equações com grau maior que 5.

Referências

[1] DOMINGUES, H. **Fundamentos de Aritmética**, Editora Atual, 1991.

[2] DOMINGUES. HYGINO, **Àlgebra Abstrata**. 1ª ed. São Paulo: Editora Moderna, 1999.

[3] SHOKRANIAN, S.; SOARES, M.; GODINHO,H. **Teoria dos Números**, 2ª ed. Brasília. Editora UnB, 1994.

[4] ALENCAR Filho, Edgard de **- Teoria Elementar dos Números/**Edgard de Alencar Filho. 2. ed. São Paulo: Nobel, 1985.

[5] POMBO, Olga. **Disputationes Arithmeticae**. Disponivel em: http://www.educ.fc.ul.pt. Acessado em: 24 de maio de 2011.

[6] **CONGRUÊNCIA, álgebra**.
Disponível em: http://pt.wikipedia.org. Acessado em: 24 de maio de 2011. John J.

[7] RICIERI, Aguinaldo P. **Karl Friedrich Gauss**.
Disponível em: http://www.miniweb.com.br/ciencias/artigos. Acessado em: 24 de maio de 2011.